Public Comments Received on

NIST SP 800-63-2:

Electronic Authentication Guideline

CertiPath, Inc.

NIST has requested public feedback on Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*, to identify areas that are deemed most significant for revision. Of the seven topic areas, CertiPath Inc. is responding to: *What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?*

At Electronic Authentication Level Four (EAL-4), identity proofing requires an in-person presence before a trusted registration authority (RA); this is not only labor and cost intensive for the identity provider, but also represents a limiting factor for wide scale deployment and effectiveness of strong identity credentials. By today's understanding of "in-person presence," a vast network of brick-and-mortar establishments is required staffed by knowledgeable personnel where applicants must *show up* with documentation in hand in order to undergo the identity proofing and registration process. This keeps costs high and participation low.

SP 800-63 makes no effort to define in-person vis-à-vis remote identity proofing. It simply states: *An Applicant may appear in person to register, or the Applicant may register remotely.* It is assumed these terms are well-understood. However, with the current state of technology, it is possible to have an in-person *face-to-face* encounter between a trusted RA and an applicant without requiring that the two individuals be in the same physical location. It involves the use of video-proofing, in a controlled environment, that connects the applicant with a manned Call Center, where he/she interacts with a trusted RA to complete the identity proofing and registration process.

This is not remote proofing, which assumes the blind submission of information/documentation from an applicant's personal computer to an identity provider's system, which may be manned or automated, but in association with which there is no exchange that constitutes a face-to-face encounter. Rather, the envisioned video proofing process is a one-on-one encounter between the applicant and the trusted RA, conducted in real time that could be deemed acceptable even for the issuance of FIPS 201 compliant PIV cards, if the SP 800-63 definition of *in-person* were expanded to include it.

There would need to be a strict set of technical requirements applied to a video proofing solution to ensure it effectively meets the written (and inferred) requirements for in-person proofing. We have identified the following criteria for a video proofing capability (there may be more):

- There must be human interaction between a live operator (trusted RA) and the applicant for the entirety of the identity proofing and registration session;
- The video feed must ensure that all actions taken by the applicant are within the field of view of the trusted RA throughout the entire identity proofing and registration session;
- The communication between the applicant and the trusted RA employs cryptography to ensure the confidentiality and integrity of the information exchanged;
- The application process utilizes biometric capture devices in accord with appropriate NIST standards; and
- The application process utilizes a document scanner that ensures high quality images for review and evaluation.

Video proofing allows for the wide deployment of in-person identity proofing locations at a fraction of the cost of a traditional brick-and-mortar presence, and the aggregation of trusted RAs at a single location increases the efficiency of the registration process.

In order to make the kiosk approach viable for *in-person registration* in the context of SP 800-63, Section 5.1 of the current document must be modified to extend the definition of in-person to include the video proofing scenario. Please see the attached proposed language modification.

Proposed Change to SP 800-63-2 Section 5.1 (new language is in Red)

In the registration process, an Applicant undergoes identity proofing by a trusted RA. If the RA is able to verify the Applicant's identity, the CSP registers or gives the Applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The Applicant is now a Subscriber of the CSP and may use the token as a Claimant in an authentication protocol. This section describes the requirements for registration and for token and credential issuance.

The RA can be a part of the CSP, or the RA can be a separate and independent entity; however, a trusted relationship always exists between the RA and CSP. The RA or CSP maintain records of the registration. The RA and CSP can provide services on behalf of an organization or may provide services to the public. The processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA operates on behalf of an organization, the identity proofing process may be able to leverage a preexisting relationship (e.g., the Applicant is an employee or student). Where the RA provides services to the public, the identity proofing process is generally limited to confirming publicly available information and previously issued credentials.

The registration and identity proofing processes are designed based on the required assurance level, to ensure that the RA/CSP knows the true identity of the Applicant. Specifically, the requirements include measures to ensure that:

- A person with the Applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The Applicant whose token is registered is in fact the person who is entitled to the identity;
- It is difficult for the Claimant to later repudiate the registration and dispute an authentication using the Subscriber's token.

An Applicant may appear in person to register, or the Applicant may register remotely. Somewhat different processes and mechanisms apply to identity proofing in each case:

In-person registration has traditionally assumed that the applicant and the trusted RA are participating in a face-to-face encounter; however, an in-person registration may also be enabled through the use of video-proofing provided all of the following criteria are met:

- Video proofing constitutes a human "face-to-face" interaction between a live operator (trusted RA) and the applicant for the entirety of the identity proofing and registration session ;
- All actions taken by the applicant are within the field of view of the video feed as one continuous image throughout the entire identity proofing and registration session;

- The communication between the applicant and the live operator employs cryptography to ensure the confidentiality and integrity of the information exchanged;
- The video proofing application process utilizes biometric capture devices in accord with appropriate NIST standards; and
- The video proofing application process utilizes a document scanner that ensures high quality images for review and evaluation.

Remote registration assumes the applicant is submitting information to an automated system for off-line processing. Remote registration is limited to Levels 1 through 3.

After successful identity proofing of the Applicant, the RA registers the Applicant, and then the CSP is responsible for token and credential issuance for the new Subscriber (additional CSP responsibilities are discussed further in Section 7). Issuance includes creation of the token. Depending on the type of token being used, the CSP will either create a new token and supply the token to the Subscriber, or require the Subscriber to register a token that the Applicant already possesses or has newly created. In either case, the mechanism for transporting the token from the token origination point to the Subscriber may need to be secured to ensure that the confidentiality and integrity of the newly established token is maintained and that token is in possession of correct Applicant.

The CSP is also responsible for the creation of a credential that binds the Subscriber's identity to his or her token. Optionally, the CSP may include other verified attributes about the Subscriber within the credential, such as his or her organizational affiliation, policies, or constraints for token use.

In models where the registration and identity proofing take place separately from credential issuance, the CSP is responsible for verifying that the credential is being issued to the same person who was identity proofed by the RA. In this model, issuance must be strongly bound to registration and identity proofing so that an Attacker cannot pose as a newly registered Subscriber and attempt to collect a token/credential meant for the actual Subscriber. This attack, and similar attacks, can be thwarted by the methods described in Section 5.3.1 (below Table 3), which describes which techniques are considered appropriate for establishing the necessary binding at the various assurance levels.

On June 29, 2015, we will be demonstrating a video proofing capability using a kiosk specifically designed to satisfy the SP 800-63 requirements for in-person identity proofing as follows:

SP 800-63 Text	Video Proofing
In-person appearance and verification of: *a)* a current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., driver's license or passport), and; *b)* either a second, independent Government ID document that contains current corroborating information (e.g., either address of record or nationality of record), OR verification of a financial account number (e.g., checking account, savings account, loan or credit card) confirmed via records.	At the start of the kiosk session, A connection is established with a Trusted RA featuring skills and language based agent routing. The kiosk provides real time audio & video conferencing between the Trusted RA and the enrollee. The Trusted RA inherits control of the kiosk Application. The kiosk Scene camera is provided to support Trusted RA presence, situational awareness, enrollment process video archival, and surveillance.
Primary Photo ID: ***RA*** inspects photo-ID and verifies via the issuing government agency or through credit bureaus or	The kiosk includes integrated document scanners for quick and accurate identification of government-issued ID of

similar databases. Confirms that: name, DoB, address, and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number. • *Secondary Government ID or financial account* *a)* ***RA*** inspects secondary Government ID and if apparently valid, confirms that the identifying information is consistent with the primary Photo-ID, or; *b)* ***RA*** verifies financial account number supplied by Applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. **[Note: Address of record shall be confirmed through validation of either the primary or secondary ID.]** • *Current Biometric* ***RA*** records a current biometric (e.g., photograph or fingerprints) to ensure that Applicant cannot repudiate application. • *Credential Issuance* ***CSP*** issues credentials in a manner that confirms address of record.	multiple sizes. By performing a variety of forensic-quality tests specific to the type of document, the kiosk can recognize and authenticate over 2,500 different types of ID documents such as passports, visas, driver's licenses, military IDs, alien registration cards, and federal, state, and local government IDs from all over the world. The full page A4 document reader uses multiple wavelength illumination — visible IR, UV, 3M™ Confirm laminate, RFID — technology to read and authenticate multiple document types quickly, easily and accurately. A ruggedized, high-resolution, duplex scanner that uses multiple light sources to provide comprehensive screening of any ID1-sized document. Reads and extracts data from front and back of ID including barcode and magstripe in a single scan. The Kiosk utilizes FIPS 201 APL Certified biometric capture devices and algorithms for the production of biometric templates and imagery.
At Level 4: Only physical transactions apply. The Applicant shall identify himself/herself in person in each new physical transaction through the use of a biometric that was recorded during a prior encounter. If the CSP issues permanent secrets, then they shall be loaded locally onto a physical device that is issued in person or delivered in a manner that confirms the address of record.	
If the RA and CSP are remotely located and communicate over a network, the entire registration transaction between the RA and CSP shall occur over a mutually authenticated protected session. Equivalently, the transaction may consist of time-stamped or sequenced messages signed by their source and encrypted for their recipient. In either case, Approved cryptography is required.	Endpoint to Server Security - All communications between system endpoints and the servers are encrypted using SSL.

The video-proofing kiosk allows for the wide deployment of in-person identity proofing locations at a fraction of the cost of a traditional brick-and-mortar presence, and the aggregation of trusted RAs at a single location increases the efficiency of the registration process.

In order to make the kiosk approach viable for *in-person registration* in the context of SP 800-63, Section 5.1 of the current document must be modified to extend the definition of in-person to include the video proofing scenario. Please see the attached proposed language modification.

Proposed Change to SP 800-63-2 Section 5.1 (new language is in Red)

In the registration process, an Applicant undergoes identity proofing by a trusted RA. If the RA is able to verify the Applicant's identity, the CSP registers or gives the Applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The Applicant is now a Subscriber of the CSP and may use the token as a Claimant in an authentication protocol. This section describes the requirements for registration and for token and credential issuance.

The RA can be a part of the CSP, or the RA can be a separate and independent entity; however, a trusted relationship always exists between the RA and CSP. The RA or CSP maintain records of the registration. The RA and CSP can provide services on behalf of an organization or may provide services to the public. The processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA operates on behalf of an organization, the identity proofing process may be able to leverage a preexisting relationship (e.g., the Applicant is an employee or student). Where the RA provides services to the public, the identity proofing process is generally limited to confirming publicly available information and previously issued credentials.

The registration and identity proofing processes are designed based on the required assurance level, to ensure that the RA/CSP knows the true identity of the Applicant. Specifically, the requirements include measures to ensure that:

- A person with the Applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The Applicant whose token is registered is in fact the person who is entitled to the identity;
- It is difficult for the Claimant to later repudiate the registration and dispute an authentication using the Subscriber's token.

An Applicant may appear in person to register, or the Applicant may register remotely. Somewhat different processes and mechanisms apply to identity proofing in each case:

In-person registration has traditionally assumed that the applicant and the trusted RA are participating in a face-to-face encounter; however, an in-person registration may also be enabled through the use of video-proofing provided all of the following criteria are met:

- Video proofing constitutes a human "face-to-face" interaction between a live operator (trusted RA) and the applicant for the entirety of the identity proofing and registration session ;
- All actions taken by the applicant are within the field of view of the video feed as one continuous image throughout the entire identity proofing and registration session;
- The communication between the applicant and the live operator employs cryptography to ensure the confidentiality and integrity of the information exchanged;
- The video proofing application process utilizes biometric capture devices in accord with appropriate NIST standards; and

- The video proofing application process utilizes a document scanner that ensures high quality images for review and evaluation.

Remote registration assumes the applicant is submitting information to an automated system for off-line processing. Remote registration is limited to Levels 1 through 3.

After successful identity proofing of the Applicant, the RA registers the Applicant, and then the CSP is responsible for token and credential issuance for the new Subscriber (additional CSP responsibilities are discussed further in Section 7). Issuance includes creation of the token. Depending on the type of token being used, the CSP will either create a new token and supply the token to the Subscriber, or require the Subscriber to register a token that the Applicant already possesses or has newly created. In either case, the mechanism for transporting the token from the token origination point to the Subscriber may need to be secured to ensure that the confidentiality and integrity of the newly established token is maintained and that token is in possession of correct Applicant.

The CSP is also responsible for the creation of a credential that binds the Subscriber's identity to his or her token. Optionally, the CSP may include other verified attributes about the Subscriber within the credential, such as his or her organizational affiliation, policies, or constraints for token use.

In models where the registration and identity proofing take place separately from credential issuance, the CSP is responsible for verifying that the credential is being issued to the same person who was identity proofed by the RA. In this model, issuance must be strongly bound to registration and identity proofing so that an Attacker cannot pose as a newly registered Subscriber and attempt to collect a token/credential meant for the actual Subscriber. This attack, and similar attacks, can be thwarted by the methods described in Section 5.3.1 (below Table 3), which describes which techniques are considered appropriate for establishing the necessary binding at the various assurance levels.

Oxford Biochronometrics

On behalf of Oxford BioChronometrics (OBC), we are pleased to offer the following comments in response to the National Institute of Standards and Technology's (NIST) request for comments on potential revisions to Special Publication 800-63-2, Electronic Authentication Guideline. (SP 800-63-2). We believe that OBC's comments on proven and developing technologies address a number of the issues raised by, as NIST noted, "market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication.1

OBC supports NIST's efforts to ensure that policy keeps pace with new technologies and we applaud NIST for aggressively seeking information regarding market innovations that may not currently be addressed in the existing guideline that may drive more secure electronic authentication (e-authentication) among those federal agencies directed by the Office of Management and Budget (OMB) to implement such standards. To be as concise as possible in an extremely complex subject we have chosen to answer 3 of NIST's questions directly.

What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

We believe that a new approach to identity proofing that utilizes the behavior of the user may allow for a much higher degree of confidence in e-authentication. We will discuss the background of this technology and its current applications so that NIST may better understand developments in the advances in biometric technology since NIST revised SP 800-63-2.

Background:

The concept of achieving transparent, frictionless and continuous identity validation in real-time through the identification of unique individual characteristics is not new. In fact, it predates the advent of computers with the first successful identification of individuals in this manner occurring in the late 1800s when individual telegraph operators were identified by their unique styles of transmitting Morse code. This process was the precursor to what we now call "Keystroke Dynamics"1. Obviously, the field of Keystroke Dynamics has progressed significantly with numerous methodologies and combinations of methodologies having evolved over time. Modern techniques that refine and adjust the analysis in real time (dynamic) to compensate for fundamental drawbacks inherent in a schema that only observes how an individual types have produced encouraging FAR, FRR, and EER results in recent years2. However, the reality is that the Biometric of Keystroke Dynamics represents only a small fraction of data points now available to achieve the true aim of transparent, frictionless and continuous identity validation.

The Innovation:

Modern electronics, particularly smart phones and computers, have expanded the available data points that can be used to identify and verify users. In what NIST might term behavioral biometrics in SP 800-63-2, "BioChronometrics"3 and similar competitive technologies with their

own terminologies for the approach, leverage keystroke dynamics as only a minor subset within 450+ factors which can be used in combination to achieve unique individual user identification. We call this dynamic combination of factors a user's "e-DNA"4 (electronically-Defined Natural Attributes). We believe this approach can result in a high level of confidence in remote identity proofing. While this approach is not specifically addressed in SP 800-63-2, we feel that, depending on interpretation, much of the existing terminology used in SP 800-63-2 may already accommodate the methodology and only minor clarifications may be needed. Our primary reason for responding to NIST's request for comment is to explain the approaches taken with this technology and to offer NIST a few points to consider when revising 800-63-2 particularly with regard to the concept of tokens and how Level 4 security might be enhanced.

General Description:

Among the 450+ factors that can be analyzed in real time5 are an array of sensory data that were either previously unavailable or, when examined separately, not strong enough indicators to authenticate identity on their own. These new approaches collect, weight and analyze all available data points6 to achieve behaviorally based identity validation. In using this approach, the data collection only occurs when the user visits a webpage or app that has the collection code embedded in it and the entire identity validation process requires nothing more than normal user/device interaction. Obviously, from a privacy perspective, this approach offers advantages in that any authentication methodology that only collects user/device interaction data and only does this from the time a user attempts to initiate a secure session through the end of the session (i.e. does not "follow" the user).

However, of equal importance, general data collection from a specific site or app (usually achieved through insertion of a small JavaScript code block) means that malicious third parties have no means of learning which factors are relevant, when and how they will be used/weighted, or even if they are to be used at all. Because so many different factors are collected, the set of device and behavioral data that are actually used cannot be determined by looking at the collection code embedded in the web site or app. Of the data set collected, perhaps only 10% (48) of collected factors may be used for authentication purposes when identifying the individual user, even though the collection of the full set of data has intrinsic security value.

Another benefit to using this methodology is that identification of the specific data elements that are used for authentication are not known outside of the BioChronometrics Authentication Database/Server. Obviously, this can be a critical element in the thwarting of any intrusion efforts. Moreover, because the values of those specific data factors (and the remaining data elements) are **not static**, this prevents a comparative analysis between prior data sets. Similarly, the subset of data elements are different for each individual, making a comparative analysis between individuals also of no value to a would-be intruder.

The following example demonstrates the above points:

Alice

QjNh WFJv SUdw RGNt bHdk QzRn VkhK NUlI Vnph VzVu SUVw VFRH bHVk

Q0Iw YnlC ellX NTBh WHBs SUhs dmRY WdTb UYyW ZOam NtbH QzRL SUVO

dmJY Qnla WE56 WldR Z09p Qlha U0J6 ZEhK dmJt ZHNl U0J5 WldO mJXM

Bob

Wxib VFnZ Edoa GRDQ jViM 1VnY ldsd WFXW jVJS Gx2Z FhJZ 1NtR jJZV

21sd 2RDQ jFjM mx1W lCdm JteH BibV VnZE c5dm JITW djM1 ZqYU CaGN

5Qkt VME5 2Ylh CeVp YTnp JRzl 5SUU xcGJ tbG1 VXBo ZG1G VFkz nBjS

In this example, each line represents a sample data set from a single authentication attempt (albeit significantly reduced in size for the purposes of this demonstration). The first block belongs to Alice and the second block belongs to Bob. The highlighted columns contain the uniquely identifying data for the respective individual.

Comparing all of Alice's prior attempts does not lead to knowledge of Alice's uniquely identifying data. Comparing Alice's prior attempts to Bob's prior attempts does not lead to knowledge of either's uniquely identifying data. Furthermore, those elements highlighted in red are valid identifying data only under certain conditions and only at a given point in time. In fact, they may not represent the same value or even have any value at all one minute later in the secure session. Thus the derived identifying "token" can be said to be non-deterministic in nature and the resultant authentication continuous.

As a result, these "fluctuating" tokens or "real time OTPs" (One Time Passwords) are orders of magnitude more difficult to hack than static ones. Another clear advantage to this approach is that even if the underlying data used to establish or confirm an e-DNA were stolen, it would have no value to the malicious third party. Without the proper algorithmic interpretation, the underlying data is essentially useless.

While there are numerous studies (several cited here) that corroborate our belief that increased confidence levels through behavioral based authentication methodologies can be achieved, we are currently in the process of independently validating the efficacy of our BioChronometric solution when used in combination with various commonly used methodologies and will furnish the results to NIST as soon as they become available. At this time, we wish only to raise NIST's general awareness regarding these advances in technology, the existing research suggesting that such an approach could greatly increase the effectiveness of existing security methodologies and that NIST specifically take such promising efforts and emergent technologies into consideration when revising SP 800-63-2.

What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

Given the above discussion on the significance and pace of recent innovations in advanced biometrics, we are requesting that NIST consider better accommodating the use of these newly available technologies7 in its future guidance and revisions. While these advancements are technically still considered biometrics and partially accommodated in SP 800-63-2, (e.g. "automated recognition of individuals based on their behavioral and biological characteristics"8), we believe current capabilities greatly exceed previous considerations of biometrics in general as well as commonly accepted notions of high assurance Multi Factor Authentication.

While there are certainly areas within existing NIST guidance language which are supportive of technologies/methodologies such as our own, there are other instances which create uncertainty, due in large part, we believe, to an understandably somewhat outmoded (given the pace of advancement we are witnessing) perception of the technologies in question. For example, we are of the opinion that current SP 800-63-2 language such as "Biometric characteristics do not constitute secrets suitable for conventional remote authentication protocols…"9 is perhaps too broad in its scope and somewhat dated in its preconceptions. As such, we would ask that such language be reconsidered or at least clarified.

In the same vein, NIST states in Section 4 of SP 800-63-2 that "In this document, e-authentication tokens always contain a secret."10 NIST adds later in the same paragraph that "More generally, something you are does not generally constitute a secret…[and] Accordingly, this recommendation does not permit the use of biometrics as a token."11 We would invite NIST to consider that the many, many factors currently used by Oxford Biochronometrics, and some of our competitors, to electronically authenticate users do constitute a secret in that the combination of these factors for any individual are unique and almost impossible to others to acquire, replicate, and deploy to hack into a system.

Moreover, NIST already recognizes the utility and security of biometrics in certain situations. Notably, NIST stated in SP 800-63-2 that "This document supports the use of biometrics to "unlock" conventional authentication tokens, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process."12 We are of the view that in light of recent advances in the use of biometrics for successfully achieving a high degree of confidence in e-authentication, NIST should consider expanding the circumstances under which behavioral biometrics could serve as a factor in authentication.

While we can certainly understand how biometrics evaluated during a previous point in time may have yielded such guidance, it is this apparent ambiguity to biometrics that we are asking NIST to address in any future guidance. Specifically, we would like to invite and participate in a dialogue with NIST regarding approaches that were likely not contemplated at the time 800-63-2 was published.

What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

As a company, we understand and strongly respect individual privacy considerations and would suggest that identity proofing methodologies such as our own (as well as that of some of our competitors) which do not rely on tracking a user's internet activity outside of a secure session are preferable to those which are often far more intrusive in nature. Specifically, we would suggest that the capabilities of advanced behavioral biometrics technology are particularly well-suited as a privacy-enhancing solution.

Because identity proofing is accomplished through analyzing user/device interaction only at the time they are interacting with a website or app with embedded collection code, the aforementioned "tracking" is not necessary. Also, the methodology assigns an alphanumeric identifier to a user which results in no actual names or many other types of particularly sensitive types of personal information (dates of birth, social security numbers, banking information, etc.) being required or stored. In other words, the user's personal information is not collected, they are not tracked, and there is no risk of their personal information being stolen.

Moreover, in our view, Identity Proofing vendors should be able to clearly demonstrate that data used for identity proofing is not re-used, repurposed or re-sold for additional economic gain at the cost of individual privacy.

Endnotes

1 http://en.wikipedia.org/wiki/Keystroke_dynamics.
2 "A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges" Mrs. D. Shanmugapriya & Dr. G. Padmavathi; (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009 http://arxiv.org/ftp/arxiv/papers/0910/0910.0817.pdf.
3 http://oxford-biochron.com/biochronometrics-a-look-under-the-hood/.
4 http://oxford-biochron.com/what-is-e-dna/.
5 Information transmission occurs in "pulses" that may not be a continuous stream.
6 Collection code requests all data points available irrespective of the device accessing the web site or app.
7 http://www.techradar.com/us/news/phone-and-communications/mobile-phones/sensory-overload-how-your-smartphone-is-becoming-part-of-you-1210244.
8 Page 7, Special Publication 800-63-2 "Electronic Authentication Guideline" Publication Date: August 2013, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.
9 Page 4, ibid.
10 Page 21, ibid.
11 Ibid.
12 Page 7, ibid.

IRS Online Services

Background

These comments are focused on remote identity proofing requirements for levels of assurance (LOA) 2 and 3. The IRS, like many federal agencies, provides services to a significant number of citizens. Many of these users are coming to the IRS to request access to personally identifiable information (PII) related to prior year tax returns or payment information. It is infeasible for the IRS to perform in-person identity proofing for these users, and unaffordable for the IRS to issue or manage LOA 4 credentials for these individuals. As a result, the IRS's identity proofing focus is on the requirements to adequately determine the identity of these users at LOA 2 and 3.

The IRS has found, both through its internally managed identity provider service, IRS e-Authentication, and through discussions with other identity providers, that requirements as stated in NIST SP 800-63-2 for LOA 2 and 3 identity proofing are not understood or implemented consistently, and do not address the full scope of current processes and technologies available to support identity proofing. In addition, techniques currently used may not be adequate to prevent large-scale identity fraud.

The following table provides the current text found in NIST SP 800-63-2 for remote identity proofing at LOA 2 and 3, as found in Section 5.3.1.

LOA	LOA 2	LOA 3
Basis for Issuing Credentials	Possession of a valid current government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g. checking account, savings account, utility account, loan or credit card, or tax ID) confirmed via records of either the government ID or account number. Note that confirmation of the financial or utility account may require supplemental information from the applicant.	Possession of a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via records of both numbers. Note that confirmation of the financial or utility account may require supplemental information from the Applicant
RA and CSP Actions	• RA inspects both ID number and account number supplied by Applicant (e.g., for correct number of digits). Verifies information provided by Applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are on balance consistent with the application and	• RA verifies information provided by Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. At a minimum, the records check for both the ID number AND the account

LOA	LOA 2	LOA 3
	sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) • Address/phone number confirmation and notification: *(Footnote: Requirements that use USPS mail for address confirmation and/or notification have a legal basis: Title 18 U.S. Code: Criminal Procedure, Section 1708: Theft or receipt of stolen mail matter generally)* a) CSP issues credentials in a manner that confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in records; or b) If personal information in records includes a telephone number or e-mail address, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days; or c) CSP issues credentials. RA or CSP sends notice to an address of record confirmed in the records check. *(Footnote Agencies are encouraged to use methods a) and b) where possible to achieve better security. Method c) is especially weak when not used in combination with knowledge of account activity.)*	number should confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) • Address confirmation: a) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; *(Footnote: Requirements that use USPS mail for address confirmation and/or notification have a legal basis: Title 18 U.S. Code: Criminal Procedure, Section 1708: Theft or receipt of stolen mail matter generally)* or b) If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are consistent with the information provided by the applicant, then the CSP may issue credentials in a manner that confirms ability of the Applicant to receive messages (SMS, voice or e-mail) sent to the electronic address. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days

Comments

1. Language used for LOA 2 and LOA 3 descriptions is not consistent. For requirements that are common to both levels of assurance, recommend using identical language so it is clear what the additional requirements are for LOA 3.
2. LOA 2 requires collecting both a valid government ID and a financial account number, but only requires validating one of them. Collection of information which is not validated does not meet best practices from a privacy perspective. Information that is not validated should not be required to be submitted.
3. LOA 2 lists checking account, savings account, utility account, loan or credit card, or tax ID as examples of financial accounts. However, LOA 2 does not include tax ID in the list. Was this change intentional?
4. LOA 2 lists tax ID as a financial account. However, since for most individuals their tax ID is their Social Security Number, this would seem to fall into the valid government ID category rather than the financial account category.
5. LOA 2 allows and LOA 3 requires verification of a financial account. However, agencies and commercial identity providers have had difficulty with getting users to provide financial account information and therefore end up implementing alternate techniques to substitute for financial account verification. NIST should reconsider the use of financial account verification as an identity proofing option.
6. Both LOA 2 and 3 remote identity proofing rely on the use of U.S. postal mail to confirm that the individual is able to receive mail at the listed address (LOA 2 allows this to be performed after credential issuance, while LOA 3 requires verification as part of the identity proofing). In practice, the use of U.S. postal mail adds time and cost to the identity proofing process, and many identity providers are using practices such as knowledge based authentication (KBA) to substitute for the U.S. postal mailing. Because this practice is so widespread, NIST should directly address it by stating what is and is not acceptable to meet the identity proofing requirements for LOA 2 and 3, and what can and cannot substitute for verifying the ability to receive U.S. postal mailings.
7. Both LOA 2 and 3permits the use of an email address or phone number on file to substitute for U.S. postal mail. However, no details are provided for the level of assurance for how the email address or phone number was verified when it was provided. If a fraudster is able to get an incorrect email or phone number associated with the identity during a previous transaction, then verification of this email address or phone number does not provide valid identity proofing. While the use of an email address or phone number verification could be an acceptable, guidance should be provided regarding how that information was determined prior to relying on it.
8. LOA 2 and 3 still rely on validating static user attributes, such as a government ID, financial or utility account number, address, etc. Given the high incidence of static attribute theft (e.g. SSNs being stolen), LOA 2 and 3 would do well to start including layers of identity verification and fraud detection that require verifying consumer behavior, device detection, and other anomalies.
9. Knowledge based authentication (KBA) is commonly used across industry and government to electronically verify identity. However, there are known issues with KBA where fraudsters have either hacked the databases that KBA information is based on, used social engineering and other techniques to determine the values, or outright bought the information. As a result, these fraudsters can successfully respond to KBA challenges. In addition, providers of KBA services use different scoring mechanisms to determine pass rates, which can affect the overall percentage of users who

pass, including both legitimate and fraudulent. NIST should provide specific guidelines on the use of KBA.

10. Because remote identity proofing techniques and the capabilities of fruadsters are continually changing, NIST should consider moving specifics to a web page or other guidance mechanism that can be updated more frequently than a special publication.

Zygma

From: Richard G. Wilsher

Email content:

My apologies for submitting this comment five days late. Although late, I believe it will be worthy of consideration and unlikely to be of a subject which will be made as positively in other submissions.

I have participated in the submission of a set of comments from an industry body but want to make a special plea to those who influence the style and presentation of NIST publications in general and this one in particular.

My perspective is one of implementer and assessor, and each focus comes down to the same point: poor structure in the document. It is difficult to determine which of the content of SP 800-63(-2) is general background / scene-setting and which is explicit guidance /requirements. Furthermore, there is a distinct lack of clarity / separation in the explicit requirements for the discrete Assurance Levels. Finally, the presentation of material as extensive, homogenous, paragraphs, often mixing tutorial-like material with requirements, thus further obfuscating the content, renders it very difficult to show conformity with the publication[1]s requirements, whether implementing or verifying conformity. This point will be borne out by, inter alia, the fact that FICAM has seen fit to replicate many of the requirements of 800-63-2 in its own requirements.

What a new 800-63 needs, whether it be 800-63-3 or some complete replacement, is clear, succinct and uniquely-referencable clauses which facilitate verification of implementations against the standard and the performance of conformity assessments (such as are provided under the Kantara IAF, e.g.) for those who believe they have implemented solutions using the standard as (at least a part of) their conformity target.

As an exemplar of what I mean, I attach a document which I produced on behalf of Kantara ¬ a re-structuring of 800-63-2 (this document also includes a mapping against the Kantara Service Assessment Criteria, which was the purpose of its creation, though the mapping per se is not relevant to this submission). In this restructuring I tried hard NOT to change any of NIST[1]s text, although in some instances the applied structure or grammatical considerations demanded minimal changes, which have been indicated by them being included in italics. Only those parts of the document which expressed requirements have been treated to re-structuring, although there is a case for substantial change throughout. Resources at the time did not allow that luxury. Apart from introductory sections, the re-structuring has been conducted specifically against the following clauses: §5.3, §6.3, §7.3, §8.3, §9.3.2.

I also refer NIST[1]s reviewers of these comments to Kantara[1]s Service Assessment Criteria, to the Common Criteria and to ISO/IEC 27001 for further examples of concise and uniquely-referenced requirements standards which serve well their intended audiences.

Your consideration of this late submission is appreciated, and I would be pleased to discuss with you any aspects of this submission.

Attachment content:

Identity Assurance Framework: Working Group Report (Draft) - Structured Electronic Authentication Guidelines

IAF-5463 v1.0
Date: 2013-12-11
Editor: Richard G. Wilsher
Zygma LLC

OASIS

OASIS (the Organization for the Advancement of Structured Information Standards) is pleased to provide this response from one of its technical committees to the request from the US National Institution of Standards and Technology (NIST) for feedback on NIST's announced plans to revise its SP 800-63-2.

PREFACE

Please note that this comment represents only viewpoints from the volunteer expert members of one of our relevant technical committees, the OASIS Trust Elevation TC [1]. OASIS is one of the largest and oldest global open data standards consortia, with approximately 5000 active participants representing about 500 member organizations and individual members in over 80 countries. [2] Our consortium hosts approximately 70 active technical committees, including a large number of open identity management standards projects [3] such as SAML, XACML, WSTrust, WS-Federation and the Trust Elevation committee, and closely cooperates with interagency and international standards cooperation efforts. [4] However, OASIS as a consortium does not take official positions on public policy matters. Our diverse group of industry, academic and governmental members, who contribute voluntarily to our projects, do not necessarily share the same views on all technical or policy matters, and OASIS emphatically does not speak for them all.

[1] OASIS Trust Elevation committee: https://www.oasis-open.org/committees/trust-el

[2] OASIS generally: https://www.oasis-open.org/

[3] OASIS identity management projects: http://j.mp/OASISidentity

[4] OASIS e-government standards liaisons: https://www.oasis-open.org/liaisons

The following statement represents a collaborative effort between the OASIS Trust Elevation TC, and the Question 10 (subcommittee) of Study Group 17 of the International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to NIST's 9 April 2015 solicitation. [5]
A related statement from ITU-T SG 17's Q10/17 is appended to this submission.

[5] NIST request for comments:
http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html

GENERAL COMMENTS

INTERNATIONAL SCOPE As the solicitation notes, “NIST is considering a significant update to SP 800-63-2 in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication.” Plainly that evolving threat landscape exists globally -- with significant effects on the United States domestically. Thus, any update of the Special Publication should include treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, SP 800-63-2 only addresses US domestic implementations, despite the agency’s extensive international mandates in its Organic Act, the provision of international standards status to its publications, and the global nature of the authentication challenges being faced. [6]

[6] See National Institute of Standards and Technology Act (http://www.nist.gov/director/ocla/upload/NIST-Organic-Act.pdf), and Organizations recognized according to Recommendations ITU-T A.4, A.5 and A.6 (http://www.itu.int/en/ITUT/extcoop/Pages/sdo.aspx).

ASSURANCE LEVELS AND ELEVATION The concept of Levels of Assurance (LoAs) today represents a range of trust, depending largely on the order and the context of the evaluation of related assurance tokens. For example, if an authentication attempt comes from an unexpected location, a system may require the use of several sets of tokens, even from the same LoA, in order to ensure that the required assurance level is achieved.

The OASIS Trust Elevation TC is developing specific, open-standards-bazed methodologies for additive actions to improve trust levels and mitigate risks incrementally. We recommend that NIST's assurance model explicitly recognize elevation methodologies in its scheme; and NIST may wish to participate in more detailed specification of standards-based elevation methods in open forums, including the OASIS committee.

IDENTITY REGISTERS We recommend that NIST explicitly add, to its assurance model, a concept and role of "Identity Register", as a repository that explicitly maintains the bindings between tokens and identifiers. Parties acting in that role should have specific, and perhapsheightened, privacy and security obligations, including the protection of significant stores of registration data retained for future dispute resolution, balanced with the risk-mitigation goal of minimizing instances of personally-identifiable information. The Identity Register role may also be defined to include support for federated authentication and identification, and support for credential reliability and recovery services.

MORE THAN ACCESS CONTROL We recommend that NIST describe and address identity and access management architectures functionally and at a higher level of abstraction, and explicitly separate identity management functions from access management functions.

CYBER RISK AND THREAT INFORMATION SHARING We note that SP 800-63-2 significantly addresses US federal systems for which the US Department of Homeland Security (DHS) also shares some responsiblities. DHS recently transferred several key data specifications for cyber threat intelligence sharing to a new OASIS technical committee for Cyber Threat Intelligence (CTI). [7] The Trust Elevation TC intends to collaborate closely with the CTI TC on implementations to reduce electronic authentication threats. NIST's evolution of the SP 800-63-2 model likely would benefit significantly from explicitly incorporating the availability of data and queries from cyber risk info sharing exchanges (such as those described in CTI specifications) into assurance level selections and trust elevation/risk mitigation transactions.

[7] OASIS CTI TC, STIX, TAXII: https://www.oasis-open.org/committees/cti

ADDITIONAL ELEMENTS FOR 800-63-2

NIST asks what requirements, processes, standards, or technologies, currently excluded from 800-63-2, should be considered for future inclusion.

We appreciate that NIST often harmonizes with and incorporates other relevant open standards very successfully. We recommend continued harmonization with ITU-T Recommendation X.1254 (also published as ISO/IEC 29115), [8] which includes extensions to the 800-63 framework, and in particular, with its treatment of non-human entities.

[8] ITU-T Rec. X.1254: Entity authentication assurance framework (2013): http://www.itu.int/rec/T-REC-X.1254/en

EXTENDED VALIDATION CERTIFICATES NIST's model should recognize recently-evolved, extensively-used industry techniques such as the Extended Validation Certificates (EVcerts) defined by CA/B Forum specifications [9] -- and the adaptation and additional token extensions found in ETSI TS 102 042 [10] -- as appropriate, risk-relevant means to combat threats to identity attributes and to minimize man-in-the-middle attacks. The CA/B Forum's recent inclusion of extensive trust certification provisions in their specification should facilitate the use of EVcerts for a broad array of government services.

[9] The Certification Authorities (CA)/Browser Forum, and its EVcerts specifications: https://cabforum.org/information-for-manufacturers-and-developers/

[10] ETSI Electronic Signatures and Infrastructures: Policy requirements for certification authorities issuing public key certificates (2013). See starting at page 8, and the references to EVCP (Extended Validation Certificates Policy) and EVCP+ (incorporating a secure user device): http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

BIOMETRIC TOKENS NIST's SP has declined to recognize robust use of biometrics data for authentication, even as the computing environment becomes mobile-first and device-centric. Although biometrics data mainly are used only at enrollment today, these methods can -- with the right privacy-enhancing methods and trust elevation -- can be evolved to provide effective user authentication properly recognized at higher levels of assurance, reaching (at a minimum) what is currently defined as LoA 2. (See, for example, the OASIS iBOPS project [11].) We recommend that NIST reconsider this omission, and fully recognize biometric tokens in its trust model.

[11] OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC and the working drafts posted there: https://www.oasis-open.org/committees/ibops The draft IBOPS model enables a user to authenticate to a device, and then enables an agent to attest to this fact, adding to reliability based on the verifier.

CONFIDENCE LEVELS

LEVEL CALCULATION *NIST's solicitation asks whether representations of the confidence level in attributes should be standardized, in order to assist in making authorization decisions, and what form it should take.*

At the point of transaction, it is no longer enough to evaluate the credential: the environment in which it is recieved also must be evaluated. The threat environment affects the trustworthiness of a transmitted credential. SP 800-63's coarse-grained "levels" may not be sufficiently detailed, or responsive, to support the determination of incremental changes in context-driven trustworthiness.

Many systems and devices in use today are designed to support flexible authentication, based on risk-based access and the foregoing considerations. Some of these systems select from among many tokens, from a defined assurance level, to enhance trust within a specific authentication step. NIST's model should accommodate and represent those flexible practices, and defined trust elevation methodologies, so as to leverage the existence of identity and LoA metadata and token consumption, as can be facilitated by existing data protocols such as SAML,

OAuth, OpenID Connect, etc.

The OASIS Trust Elevation TC is developing a detailed methodology, currently published in draft, for determining, indicating, evaluating and improving on assurance levels, in a technologyindependent fashion, as described below. The committee also is developing metadata structures to express, and protocols for exchanging, trust-level data and requests between verifiers and clients.

NIST also should consider assigning greater trustworthiness values to hacker-resistant authentication architectures, in cases where hacking is a significant environmental risk. For example, in IBOPS' methodology, the identity provider's server holds only a pointer to the client secrets and does not store any credentials locally; client secrets are stored on the client, which reduces the risk that hacking the identity provider will result in large-scale security breaches.

TRUST ELEVATION AND MULTIFACTOR CALCULATIONS *NIST's solicitation asks what methods can be used to increase the trust or assurance level of an authenticated identity during a transaction.*

The historical SP 800-63 framework looks at three traditional categories of authentication factors: something you have, something you are, and something you know. But these categories are limiting: they assume strict, static authentication tokens with limited authentication capabilities. In many cases, the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by an adaptive authentication engine.

NIST should enlarge the scope of authentication categories in its model, to represent the use of context and behavior, and the policy or circumstances that govern when they will be factored into an authentication decision, so to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smartphone can house a soft token that protects a soft PKI certificate in a Key Chain. The trust level in that token may be able to change, based on the device status or health (such as rooting), the presence and operation of anti-virus software, and perhaps the state messages generated by the latter. With those kinds of determinations, the assurance level achievable from the device can (and should be able to) vary with time, or as a function of various other data, including software on the device and indicia of system integrity.

TAKING THREATS TO AUTHENTICATION INTO ACCOUNT
As noted above, SP 800-63 gives inadequate treatment to biometrics. Currently it recognizes biometrics only in the context of enrollment and as second or third factors on hard tokens. In actual industry practice, however, biometrics indicators are used more broadly as part of a multi-factor scheme: for example, biometrics can bind the access request to a user, as part of a larger process performed by the verifier through the use of cumulative identity attributes that bind a device, location and behavior to an authorization request. Increasingly, the devices involved in the transaction matter; the model's implicit assumption that interactions are webbased between the user and the verifier is long obsolete. Applying those older-fashioned, browser-era methods, such as relying on cookies or unprotected tokens for single sign-on (SSO) support, to current environments may be more likely to result in insecure outcomes, given that many mobile SSO technologies are still at a relatively primitive stage.

COMBINED FACTORS AND COMPLEMENTARY VULNERABILITIES Increases to authentication assurance require the combination of authentication factors *as well as* minimalization of overlapping vulnerabilities. Enhancing assurance is not achieved solely by the number of factors; it also depends on the reduction in threats that a particular combination of factors can achieve. A method of combining factors may either reduce or increase threats from context and related vulnerabilities. The OASIS Trust Elevation TC has produced drafts, based on ITU-T X.1254 (ISO/IEC 29115), of a comprehensive list of authentication methods, and methods for computing their authentication strength, based on the vulnerabilities of each and their associated mitigation/control characteristics. We recommend that NIST consider building on this approach, with the objective of a catalog of factors and combinations that will better ensure that implementers understand (a) options for achieving strength of authentication, and (b) the multiple effects that various factors may have.

PATHS FOR TRUST ELEVATION A well-populated matrix of options for combined factor use also should readily identify paths for trust elevation -- by showing where the addition of a factor or factors will materially improve authentication strength, without introducing new compensating vulnerabilities that undermine it. Trust elevation opportunities can arise in multiple steps in an authentication workflow. For example, when a Credential Service Provider (CSP) authenticates a user coming from a smart device:

- The CSP may have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user.
- The authentication strength can be consistent with the risk engine requirements.
- If the CSP is acting as an identity provider or attribute provider, to other verifiers or relying parties, those parties can elevate the authentication strength per their own requirements; they may also be able to ask the CSP to do so on their behalf, or combine the CSP tokens into application-specific attributes, such as behavior, on their own.

Parties should have standardized means of requesting stronger assurance, as reflected in the specified transaction patterns under development by the OASIS Trust Elevation TC.

NIST may also wish to consider whether levels of assurance could be approached with an overlay/tailoring capability, similar to that described in NIST's SP 800-53. The revised 800-63 framework could describe a set of baseline assurance levels, each with a minimum set of factors and perhaps environmental or risk conditions – and each of which may be tailored as necessary, consistent with common tailoring guidance provided by the framework, to help each community of interest better meet its mission and business needs. Within each baseline level, adjustments to authentication strength could be approached using the additive approach adopted by the OASIS Trust Elevation TC as described above. Using this approach, it might be possible to compare some alternative factor combinations and transactional patterns, within a given baseline, in a deterministic or arithmetic manner, even if the "larger" steps between the baseline risk levels are not on a linear scale.

Respectfully submitted
James Bryce Clark
General Counsel, OASIS

May 22, 2015

INTERNATIONAL TELECOMMUNICATION UNION **COM 17 – LS 217 – E**
TELECOMMUNICATION
STANDARDIZATION SECTOR
STUDY PERIOD 2013-2016

This liaison statement represents a collaborative effort between the OASIS Trust Elevation TC and ITU-T Study Group 17, *Security*, in its Question 10/17, *Identity management architecture and mechanisms*, to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to its 9 April 2015 solicitation. (See http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html)

We also acknowledge and are grateful for the feedback and dialogue we enjoyed from participating experts of OASIS Trust Elevation TC, with whom we collaboratively developed this liaison statement, and who have been informed about this liaison statement.

I General comments

- As the solicitation notes, “NIST is considering a significant update to SP 800-63-2 in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication.” Plainly that evolving threat landscape exists globally - with significant effects on the United States domestically. Thus, any update of this Special Publication should include extensive treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, NIST SP800-63-2 is completely devoid of anything other than U.S. domestic implementations, despite the agency’s extensive international mandates in its Organic Act, the provision of international standards status to its publications, and the global nature of the authentication challenges being faced.1
- Levels of Assurance (LoA) today represents a range of trust depending on the order and the context of the evaluation of related assurance tokens. For example, if an authentication attempt comes from an unexpected location, a system may require the use of several sets of tokens even from the same LoA in order to ensure that the required assurance level is achieved. In many cases and in particular for knowledge based tokens. The attributes of these tokens losses value as a function of time. The advent of social media makes Knowledge Based Authentication (KBA) information public and water-down its effective use in the identification process
- Decouple Identity Binding

  - Permit identity proofing to occur after token issuance.
- Identity Register

  - Add to the model the concept of the Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that come with this role, including the protection of registration data for future dispute resolution balanced with user risk-mitigation goal

of minimizing instances of PII. The Identity Register may provide support for federated authentication and identification and credential reliability and recovery services.

- Risk Confidence Factors

- Instead of grouping assurance profiles solely as 1,2,3,4 per OMB M-04-04 requirements, permit the expression of risk confidence score with multiple factors including identity proofing, token strength, multiple factors, biometric verification, etc.

II What requirements, processes, standards, or technologies are currently excluded from NIST 800-63-2 that should be considered for future inclusion?

- NIST should treat extensively used industry techniques such as the Extended Validation Certificates (EVcerts) pursuant to the CA/B Forum specification or the adaptation and extension found in ETSI TS 102 042 as means to combat threats to identity attributes and minimize man in the middle attacks.

- Rec. ITU-T X.1254 (ISO 29115) have done an extensive extension additions to the NIST 800-063 framework and need to be taken into consideration.

III Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

- OASIS Trust Elevation TC has developed three committee drafts that can be used for developing a consistent method for determining, evaluating and improving on LoA levels in a technology independent fashion. It is also developing metadata and protocol for expressing and exchanging needed trust elevation methods between a verifier and a client.

1 *See* National Institute of Standards and Technology Act, [available at http://www.nist.gov/director/ocla/upload/NISTOrganic-Act.pdf. *See also*, Organizations recognized according to Recommendations ITU-T A.4, A.5 and A.6, http://www.itu.int/en/ITU-T/extcoop/Pages/sdo.aspx.

- Many systems are designed to support flexible authentication based on risk-based access. In many cases, these systems select many tokens from a given LoA to enhance the trust with the authentication step. NIST needs to be flexible and adapt the work from OASIS Trust Elevation TC in order to piggy-back on the use of common LoA metadata and trust elevation protocols that could work with IETF Oauth, OpenID Connect and OASIS SAML.

- At the point of transaction, the environment needs to be evaluated, not just the credential. NIST needs to start accommodating the latest trends in using a device as part of the authentication process. In this regard, the OASIS Identity-Based Attestation and Open Exchange Protocol Specification (IBOPS) models of enabling the user to authenticate to a device, and then an agent to attest to this fact, changes the dynamics of determining the LoA and the verifier (or CSP). Emphasis should be given to methods that lead to a hacker resistant authentication method where hacking the identity provider server will not result in massive security breaches. For example, in the OASIS Identity Based Attestation TC (IBOPS) models, the server holds a pointer to the client secrets and does not store any credentials locally. Client secrets are stored on the client device. This changes the attack vector of hackers whereby they will need to hack the server and the associated device to obtain a credential.

- Recommend harmonizing NIST SP 800-63 with work done in Rec. ITU-T X.1254, ISO 29115 and OASIS TRUST Elevation.

IV What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

- NIST SP 800-63 framework looks at the traditional three categories of authentication factors: something you have, something you are, and something you know. These categories are limiting because they assume strict and static authentication tokens with limited authentication capabilities. In many cases the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by an adaptive authentication engine. NIST needs to enlarge the scope of authentication categories to include context and behaviour to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a key chain. The trust level in the token can change based on the device health such as rooting or the use of anti-virus software. As such the achievable LoA from the device can vary with time and could be a function of software on the device and also a function of OS system integrity.
- The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrolment and second or third factors on hard tokens. However, the trend in the industry is to unlock devices using biometrics with the task of binding the access request to a user to be performed by the verifier through the use of cumulative identity attributes that binds a device, location and behaviour to an authorization request.
- The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current trends. Given that mobile single sign technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign On support.

V Threats to Authentication

- Increasing authentication assurance requires the combinations of authentication factors with no or minimal overlapping vulnerabilities can result in enhanced assurance. It is not the number of factors that matters but the reduction in threats that the combination of factors achieves. The way the combination occurs can either reduce or increase threats of context and related vulnerabilities. The OASIS Trust Elevation TC produced two committee drafts based on Recommendation ITU-T X.1254 (ISO 29115) that include a comprehensive list of authentication methods, and a way of computing the authentication strength based on vulnerabilities and their associated control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
- It is recommended that Trust Elevation techniques should be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a Credential Service Provider (CSP) can authenticate a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user.

The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per their own requirements and may be able to ask the CSP to do it on their behalf or combine the CSP tokens into application specific attributes, such as behaviour, that they also can do on their own.

- A standardized means of asking for higher assurance such as the ones being developed by OASIS Trust Elevation TC should be used.
- An overlay/tailoring capability similar to NIST SP 800-53 could also be used. Each NIST SP 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. In the overlays authentication strength can be computed using concepts form OASIS Trust Elevation TC.

VI Elevation of Biometric to a token

NIST does not recommend the use of biometrics as tokens. They are mainly used at enrolment. However, if the right privacy enhancing methods is used combined with appropriate trust elevation methods (like in OASIS IBOPS) biometric can be evolved to provide effective user authentication at least at LoA 2. So it is recommended that NIST investigate the use of biometric as a full token.

References: 4

1. OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC; https://www.oasis-open.org/apps/org/workgroup/trust-el/
2. OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC; https://www.oasis-open.org/apps/org/workgroup/ibops/
3. Recommendation ITU-T X.1254: Entity authentication assurance framework; http://www.itu.int/rec/T-REC-X.1254
4. Question 10/17 – Identity management architecture and mechanisms; http://www.itu.int/en/ITUT/studygroups/2013-2016/17/Pages/q10.aspx

BIO-key

From: Jim Sullivan

I appreciate the opportunity to comment on the SP 800-63-2 document. I echo the comments made by Cathy Tilton of Daon, as well as the comments of the IBIA, but want to add some specific comments as well.

Currently, NIST SP 800-63-2 states (emphasis added):

Biometric characteristics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document either. In the local authentication case, where the Claimant is observed by an attendant and uses a capture device controlled by the Verifier, authentication does not require that biometrics be kept secret. This document supports the use of biometrics to ³unlock² conventional authentication tokens, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process.

COMMENTS:

I. BIOMETRICS SHOULD BE ALLOWED AS A REMOTE AUTHENTICATION FACTOR

The current 800-63-2 position on biometrics appears to adopt a common, but in my opinion, mistaken, view - that secure remote biometric authentication can only be achieved by maintaining absolute secrecy of the underlying biometric data, and consequently assigns a phantom vulnerability to biometrics based on its inherently public subject matter ¬ the genuine Claimant. A commonly repeated misunderstanding along these lines is that an imposter Claimant possessing a genuine Claimant¹s fingerprint could simply present that fingerprint as part of a remote authentication sequence, as if it were acceptable as an attachment to an email, e.g. ³Hello. I¹m John Doe, and I¹ve attached his fingerprint to this email to prove it.² Passwords are indeed vulnerable in this way ¬ knowing a genuine Claimant¹s password easily allows an imposter to present it as his own using only a keyboard. Biometrics, on the other hand, are derived from a different source ¬ they are measurements of a real person. The Claimant¹s finger is the credential, not the fingerprint it leaves behind.

The fact that a biometric authentication is rooted in the repeatable measurement of a real person ¬ just like height and weight, but much more detailed, is overlooked by many critics of biometrics, who cite the well-worn concern that a biometric cannot be revoked if compromised, focusing on the phantom vulnerability cited above. In fact, it is exactly that immutability of biometric measurements that makes biometrics such a good long term authentication factor ¬ only one person has the finger, even if the whole world knows what the fingerprint looks like. The integrity of the capture, transmission and storage process, not the secrecy of the data, makes biometrics work as a remote authentication factor, and the document should detail what a well-designed system must employ to ensure the integrity of the authentication process, including liveness and anti-spoofing measures in scanners, secure transport of data between client and server, and tamper-proof storage of the vetted enrollment data, as was incorporated into the DEA EPCS regulations in CFR 21 part 1311.

II. BIOMETRICS PREVENTS IDENTITY SHARING

An often overlooked benefit of biometrics as a remote authentication factor is in the prevention of [3]identity sharing.[2] The most strong authentication protocols assume that a credential holder has an absolute interest in protecting his or her authentication credential against use by others, but overlooks the reality that an individual may cooperate with an imposter to either share an authentication protected benefit, such as a subscription or health care access, or to have a proxy or assignee perform his obligations, such as a taking a high stakes exam. The existing 800-63-2 document captures some of these benefits for consistency throughout registration and non-repudiation, but could go further to highlight that biometrics is really the only means to protect against identity sharing.

III. RECONSIDER SWIPE AND OTHER NON-PIV SCANNERS UNDER SP 800-76

Given the importance of an inclusive, cost-effective biometric approach, there should be a pathway to include non-PIV sized fingerprint capture devices as acceptable acquisition devices. A suggestion would be to provide a means for an algorithm and a specific swipe or small area sensor to be independently tested as a combination to show required accuracy levels can be met. Since many other regulations incorporate SP 800-63 and SP 800-76 by reference, having mobile-ready, lower cost form factors for scanners becomes critical.

Thanks for your consideration, and best of luck in aggregating the many ideas into your next version.

Regards,

Jim Sullivan

LexisNexis Risk Solutions

LexisNexis Risk Solutions is pleased to respond to the National Institute of Standards and Technology (NIST) regarding comments on Special Publication 800-63-2 (SP 800-63-2), *Electronic Authentication Guideline*. LexisNexis Risk Solutions (LexisNexis) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cuttingedge technology, unique data and advanced analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy.

LexisNexis offers identity proofing solutions that have been certified by SAFE-BioPharma under FICAM Trust Framework 1.0 for use in NIST SP 800-63-2 Identity Proofing Levels of Assurance 1, 2 and 3. Our identity verification and authentication products can be used in a variety of combinations to help our customers address both their specific business process needs and meet the proofing guidelines found in SP 800-63-2.

Based on our extensive experience with identity proofing for government and commercial organizations that leverage the guidance from SP 800-63-2, we provide the following set of comments:

> (1) NIST Special Publication 800-63 was initially published in 2006 to help federal agencies respond to identity proofing and authentication challenges. Over the years, it has received two updates since originally being published, most recently in August 2013 and renamed to SP 800-63-2. In practical use of SP 800-63-2, it has been our observation that customers sometimes find it difficult to understand the different options that can be used to meet the identity proofing requirements. While the identity proofing requirements are found primarily in Table 3, additional guidance has been added after this table with each publication update. Without a reference in Table 3 that links this additional guidance on fulfilling the identity proofing requirements, it can be overlooked or misunderstood.
>
> For example, the guideline states that remote registration at both Levels 2 and 3 require confirmation of a financial or utility account number. Additional guidance is provided to allow for the use of a cellular or landline telephone service account under specific conditions detailed in SP 800-63-2. Since this additional guidance is found after the Level 4 details of Table 3, it is often overlooked by those less familiar with the current version of the guideline.
>
> To improve the usability of the identity proofing guidance in SP 800-63-2, we recommend that reference be made in Table 3 to all approved methods to meet the requirements for each level of assurance and/or additional text be provided following Table 3 that details all of the approved methods to meet the requirements for each level of assurance.
>
> (2) The use of multiple factors of authentication is a well-established and increasingly adopted approach to strengthening the authentication processes used by organizations. SP 800-63-2 also references that implementations that use multiple factors of authentication improve security over fewer factors. Combining knowledge-based (“something you know”), possession-based (“something you have”), and/or biometric-based (“something you are”) factors to achieve authentication is considered to be more effective than any of the same factors used alone.
>
> Best practices from analysts firms such as Gartner have supported the notion that successive

layers in identity proofing, similar to the multiple factors of authentication, provide stronger protection and make it harder for unauthorized persons to compromise the account registration process. No singular identity-proofing method used on its own is sufficient to address the concerns of impersonation threat when higher levels of assurance are needed.

The current requirements for identity proofing in SP 800-63-2 have been designed to prevent repudiation during the registration process and mitigate impersonation threats – a) that a person with the claimed identity exists and b) that the applicant is the person who is entitled to the claimed identity. Verification of identity attributes against agency or third-party databases is an effective method to determine that a claimed identity exists; however, verification alone does not confirm that the applicant is the person who is entitled to the claimed identity. User-interaction centered techniques that directly interact with the claimant in two-way communication have proven to be more effective than verification of identity information in determining entitlement or ownership of the claimed identity. Such methods include dynamic knowledge-based authentication and phone verification combined with verification of receipt of a one-time password sent by voice or SMS.

SP 800-63-2 currently provides guidance to agencies that they may choose to use additional knowledge based authentication methods to increase confidence in the registration process once the minimum registration requirements for an assurance level have been met. In order to mitigate the impersonation threat that the applicant is not the person who is entitled to the claimed identity, we recommend requiring a user-interaction centered technique at Level 3 in addition to identity verification.

We appreciate the opportunity to respond to this Call for Comments and look forward to engaging in ways to help improve electronic authentication guidance as this process continues.

InCommon

In surveying the Higher Education community, the primary concern articulated is that the structure of the NIST LoAs ¬ and by extension, the InCommon profiles ¬ is monolithic and does not map well to the business challenges commonly experienced in Higher Education. An approach that allows for the decoupling of identity proofing and credential quality would support more use cases and likely spur more adoption.

On behalf of InCommon, we strongly encourage you to adjust the composition of the LoA in 800-63 to allow more flexibility in this regard.

Microsoft Research & Carleton University

From: Cormac Herley & Paul C. van Oorschot

We welcome the opportunity to comment. We would like to suggest that any revision bear in mind the following.

While stronger authentication and identity assurance may be on the way, many have under-estimated the difficulties of replacing passwords [1]. We encourage updating the portion of the document that pertains to plain old passwords.

We suggest that the measures of entropy recommended in the document have been shown to be seriously flawed [2,3]. Recent large-scale breaches have allowed work based on the actual guess-resistance of user-chosen secrets rather than models.

We suggest that the efficacy of composition rules be re-examined; data now shows that these rules are far less effective than is generally believed [4]. This is important, as many sites appear to rely on rules that are giving a false sense of security. Table A.1 in 800-63-2 currently examines the cases of: no checks, dictionary and dictionary + composition rules. It is worth pointing out that composition rules alone (i.e. without dictionary (aka blacklist or forbidden list)) are of doubtful efficacy (since this appears a common use case).

We suggest that the efficacy of expiring credentials be examined. Recent work has shown that new user-chosen secrets greatly resemble old after a forced credential expiration [5], and that the measure does little to make an attackers job harder [6].

We suggest that recommended protections explicitly state assumptions and expectations, e.g. whether the goal is to withstand online or offline guessing attacks. There is a significant risk of wasting user effort if measures are employed that exceed what is necessary to survive online attack but fall far short of what is necessary for offline [4].

References:

[1] C. Herley and P.C. van Oorschot, "A Research Agenda Acknowledging the Persistence of Passwords," IEEE Security and Privacy magazine, Jan. 2012.

[2] M. Weir, S. Aggarwal, M. Collins, H. Stern, Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords, Proc. ACM CCS 2010

[3] J. Bonneau, The science of guessing: analyzing an anonymized corpus of 70 million passwords, Proc. IEEE Security&Privacy 2012.

[4] D. Florencio, C. Herley and P.C. van Oorschot, "An Administrator's Guide to Internet Password Research", Proc. Usenix LISA, 2014

[5] Y. Zhang, F. Monrose, M.K. Reiter, The security of modern password expiration: an algorithmic framework and empirical analysis, Proc. ACM CCS 2010

[6] S. Chiasson, P.C. van Oorschot. Quantifying the Security Advantage of Password Expiration Policies. Designs, Codes and Cryptography, April 2015

Identity Ecosystem Steering Group (IDESG)

COMMENTS OF THE IDENTITY ECOSYSTEM STEERING GROUP (IDESG)

The Identity Ecosystem Steering Group (IDESG) welcomes the opportunity to submit comments to the National Institute for Standards and Technology (NIST) regarding SP 800-63-2, Electronic Authentication Guideline (Guideline) 1. The IDESG applauds the Director for soliciting public feedback to identify areas that industry and government feel are necessary to update and strengthen the Guideline. As explained below, the IDESG has great confidence that the Director will recognize how incorporating the principles identified in the National Strategy for Trusted Identities in Cyberspace (NSTIC) 2 into the Guideline will strengthen identity management practices government-wide. In addition, it will provide users with the confidence that their credentials, whether government-issued or issued by a third-party for government acceptance, will be protective of their privacy and security. This effort to ensure that sensitive data are shared only with the appropriate person or people is specifically supported by Executive Order 13681, Improving the Security of Consumer Financial Transactions, issued by the Obama Administration in October 20143. We are confident that an updated Guideline which incorporates the NSTIC principles consistent with the Executive Order will result in strengthened identity credentials that enhance privacy, security and usability, as well as increased consumer confidence that the online transactions they engage in with their identity credentials will deter misuse of their data, online fraud, and identity theft.

INTRODUCTION

The IDESG, a voluntary public/private partnership, is the only independent body dedicated to redefining how people and organizations identify themselves online by fostering the creation of privacy-enhancing trusted digital identities. The IDESG works to bring all netizens – consumers, educational institutions, online businesses, and governments alike – into the thriving marketplace for strong, secure online identity credentials. The heart of the IDESG's efforts is the development of the Identity Ecosystem Framework (IDEF), a protective array of standards, best practices and agreements that all IDESG participants pledge they'll adhere to. What makes this different than any effort that has come before is that the IDEF's baseline requirements are wholly grounded in the NSTIC Guiding Principles.

1 NIST Special Publication 800-63-2, Electronic Authentication Guideline, issued August 2013.

2 The National Strategy for Trusted Identities in Cyberspace, issued April 15, 2011.

3 Executive Order 13681, Improving the Security of Consumer Financial Transactions, issued October 17, 2014.

Developed at the behest of President Barack Obama in April 2011, the NSTIC originally envisioned an online environment where individuals can choose from a variety of credentials to use in lieu of passwords for interactions conducted across the internet. To satisfy the NSTIC – and pass muster with the IDESG's high standards – all identity solutions must be:

- Privacy-enhancing and voluntary;
- Secure and resilient;
- Interoperable; and
- Cost-effective and easy to use.

Initiated with the support of NIST, the IDESG is transitioning into a self-sustaining organization that will develop and administer the IDEF, oversee certification of its participants, and work to encourage world-wide adoption of these more trusted online identity credentials.

The IDESG is private-sector led and comprised of a diverse group of stakeholders, from regulated industries and IT infrastructure developers to consumer advocates, educational organizations and civil liberties groups. The IDESG's working groups and committees are realizing the goal of building an IDEF that can best meet all stakeholder needs with regard to privacy, security, and usability. IDESG membership is open to any individual or organization interested in crafting a framework for identity solutions. Membership in the IDESG tops 200 organizations, both private and public, and is truly global in scope with members representing more than 12 countries. We encourage you to visit our website at www.IDecosystem.org.

DISCUSSION

The Electronic Authentication Guideline, NIST SP 800-63-2, provides technical guidance for Federal agencies implementing remote electronic authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. The IDESG's Identity Ecosystem Framework addresses the privacy and security of the user data on the electronic credentials that are used on government IT systems, as well as those on private sector systems.

Just as adherence to the Guideline gives confidence to consumers of the credential that the user is who they say they are, holders of these identity credentials need confidence that during the authentication process the data on the credentials are being used in a manner that is transparent and protective of their privacy and security. Further, credential holders need confidence that the consumers of their identity credentials will use them in a way that does not put them at risk for identity theft, fraud, or misuse. Most importantly, credential holders need confidence that the attributes and information associated with their electronic identity credential will be used only for the purposes stated, and nothing more.

The NSTIC charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices in online transactions. In addition, the NSTIC calls for the Federal Government to "lead by example and implement the Identity Ecosystem for the services it provides internally and externally."4 The Identity Ecosystem envisioned in the NSTIC and being developed by the IDESG answers this call. The Identity Ecosystem is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information while they are conducting transactions.

4 NSTIC, pg. 37.

While the IDESG's development of baseline functional requirements for Identity Ecosystem credentials is a private-sector led effort, its underlying mission is directly supported by the White House. To wit, Executive Order 13681, Improving the Security of Consumer Financial Transactions, issued in October 2014 requires "…that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate"5, and is "consistent with the guidance set forth in the 2011 National Strategy for Trusted Identity in Cyberspace."6

Updating the Guidance for the Future

As currently written, the Guideline describes for implementing agencies the technical requirements for the four levels of assurance in:

- Identity proofing and registration of applicants,
- Tokens for authentication,
- Token and credential management mechanisms used to establish and maintain token and credential information,
- Protocols used to support the authentication mechanism between the claimant and the verifier, and
- Assertion mechanisms used to communicate the results of a remote authentication if results are sent to other parties.7

Although it was last updated in August 2013, the Guideline offers no guidance as to how implementing agencies would incorporate the NSTIC principles into the electronic authentication process.

Increasing incidents of global-scale data breaches and identity thefts have created a demand for identity credentials that are more protective of personal privacy and security, yet easy-to-use, inexpensive, and interoperable across platforms. This has been recognized by the Federal Government not only by the NSTIC in 2011, but also by the President's October 2014 Executive Order, as noted above.

If the Guideline is to remain as authoritative, relevant, and useful in its second decade of direction as it was in its first, it must be updated to incorporate the guidance set forth in the NSTIC, and require its adherence by all who would follow the Guideline¸ whether they are a public or private sector actor.

Currently, the IDESG is developing a trust framework and certification program that will assist implementers to adhere to the NSTIC principles and guidance, throughout all stages of the identity management process, including electronic authentication. This guidance is called the Identity Ecosystem Framework (IDEF). The IDEF describes methods, standards, baseline requirements and best practices in a technology-neutral manner that makes it applicable across all platforms and tools used for identity management.

5 Executive Order 1368, Section 3.

6 Ibid.

7 NIST SP 800-63-2, vi.

The IDESG believes that any further update to NIST's Electronic Authentication Guideline must:

- Incorporate requirements throughout the entire electronic authentication process consistent with the NSITC's vision of the Identity Ecosystem;
- Require implementing agencies to ensure all new and existing Federally-created credentials be certified as being aligned with the NSTIC, expressed through the use of the IDEF; and
- Require all third-party electronic credentials created by commercial companies and organizations that may be consumed by the Federal Government, its agencies, and departments, to be certified as being aligned with the NSTIC, expressed through the use of the IDEF.

An independent organization, the IDESG was initiated by the Federal Government as a public/private partnership to develop an NSTIC-compliant framework, as well as guidance to address the very issues

raised by the Administration back in 2011. As such, the continuing development of the IDEF and its requirements embody the very heart of the NSTIC principles and is an appropriate tool to assist Federal agencies and private organizations comply with future NSTIC requirements in the next update of the Electronic Authentication Guideline.

The IDESG understands this occasion to offer comments is only the first step in a necessarily involved and thorough process to outfit the Electronic Authentication Guideline for its next decade of service. The IDESG thanks you for this opportunity to comment, and looks forward to working with NIST as the process continues, remaining ready to assist in any manner it can.

If you have any comments or questions, please feel free to reach us through our Executive Director, Marc-Anthony Signorino.

Microsoft

Microsoft appreciates the opportunity to review and comment on the "Draft NIST Special Publication 800-63-2, Electronic Authentication Guideline." As a devices and services provider, we remain committed to collaborating with our government partners to create a dynamic and stronger form of identity, which is one of the greatest challenges faced in online computing.

As stated in the NIST request for comment, on Electronic Authentication Guideline, several factors have contributed to the need to update/revise the Special Publication 800-63-2, published in August 2013. Among these factors are market innovations leading to newer more secure open authentication based solutions. These market innovations are in response to a dynamically evolving threat landscape and the subsequent remote authentication compromises.

Microsoft recommends the NIST Electronic Authentication Guideline be based on a dynamic and flexible set of principles that can accommodate newer technologies for secure remote authentication, both now and in the future. One such example is the expression of assertions based on OAuth (an open standard for authorization). Microsoft proposes the use of OAuth as an acceptable federation protocol.

Microsoft also recognizes that each organization has unique needs for online remote authentication. A careful and thorough evaluation of these needs helps an organization determine their risk level, which in turn guides their assurance level requirements for their implementation strategy. Static levels of assertion, defined in terms of a hierarchical structure of LoA 1, 2, 3 and 4, are rigid and must be ductile to meet the evolving landscape. Microsoft welcomes NIST's efforts to revisit and update the levels of assurance. The LoA model going forward should reflect not only the risk level mitigation, but also the cost of implementing a particular solution. For example, it may not be necessary in all scenarios to require smartcard based authentication, instead an industry standard federation protocol supported solution may be more than appropriate and address the particular risk level being mitigated. The new NIST Electronic Authentication Guideline should be flexible and dynamic enough to allow organizations to keep pace with market innovation and the threat landscape.

Finally, Microsoft recognizes the opportunity to update the NIST 800-63-2 framework as one that could foster international adoption of a common dynamic framework for electronic authentication. NIST should also consider evolving the ISO 29115, into an international standard framework for managing entity authentication assurance in a given context.

We offer the following specific comments for your consideration.

1) **What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?**
   - ITU-T X.1254 (ISO 29115) has prepared extensive additions to the 800-63 framework. They should be taken into consideration in the current update of the Electronic Authentication Guideline. This will help ensure a more common international standard that also benefits the US public and private sector customers.
   - NIST should also consider technologies like FIDO (FIDO 2.0) and the concept of authentication via cryptography and devices in order to address the modern threat landscape and electronic

authentication protection requirements.

2) **Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?**
   - As stated earlier in this response, Microsoft recommends a more flexible and dynamic approach to assurance level determination, rather than the traditional standardized definitions used in 800-63. The determination of an appropriate confidence level will be a jurisdiction and risk factor decision based on an organization's risk level and mitigation requirements.
   - NIST should consider harmonizing the NIST SP 800-63-2 update exercise with work already done in ITU-T X.1254, ISO 29115 and to an appropriate extent ISO 29003 (Identity Proofing and the levels of proofing established in the specification).

3) **What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.**
   - There are other factors such as "signals" that can be used. Many of these signals are used for fraud and malware detection, and thus readily available from different sources.

4) **What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?**
   - Microsoft recommends the work already done by organizations like FIDO. Their (FIDO's) privacy principles should be adopted for the authentication framework, in the updated 800-63-2. Another example of privacy-enhancing technologies that NIST should consider is Attribute-Based Credentials for Trust (ABC4Trust).
   - From an identity assurance standpoint, NIST should take a look at the ISO 29003 (Identity Proofing) and the levels of Identity Proofing that have been established relative to the Levels of Authentication Assurance.

We acknowledge and commend NIST's open and collaborative process in consistently partnering with industry. We look forward to our continued engagement throughout this important initiative.

MITRE

These comments are from Jim Thomson, MITRE. They do not represent a consolidated, official MITRE position. They do, however, represent the view of certain Federal organizations as represented by MITRE. Thank you for the opportunity to comment.

Section	Page	Comment
Overall	Overall	While some have sought to reduce the LOA complexity because of its lack of use, this would be a mistake at this time. The lack of use within the federal government communities has simply been a matter of ICAM maturity. Most departments and agencies are still establishing enterprise-wide authentication systems for their own users focusing on issuing PIVs and PK-enabling systems, and have not yet been able to get to the point of dealing with various authentication methods. As internal users become more and more mobile and as departments engage with external users in compliance with EO 13681, 800-63-2 will become more and more important. So rather than minimize the complexity of LOA from four levels to three or two, as has been suggested, it's worth contemplating both adding additional considerations, such as device identity, and increasing LOA resolution for RPs who may want it. However, most RPs will want LOA to be simple. In addition, the all-or-nothing model will have to give way to reduced access; the mobile user will demand at least some access when away from her LOA 4 reader.
2. Introduction	1	While 800-63-2 conforms to OMB M-04-04 where both assume that a system has a fixed assurance level (1-4), emerging RAdAC concepts and agency needs suggest that departments and agencies will want to accept a range of authentication assurances and throttle access based on LOA. The Policy & Standards Tiger Team (PSTT) sponsored by the ICAMSC and reporting to OMB will be looking at M-04-04 in 2015 and it is reasonably likely that it will be modified to allow more flexibility. 800-63-2 should also acknowledge this concept.
4. E-Authentication Model	17	"As part of authentication, mechanisms such as device identity or geo-location could be used to identify or prevent possible authentication false positives. While these mechanisms do not directly increase the assurance level for authentication …" Device identity does increase the assurance level of authentication (something you have), particularly if it is pre-established with the CSP, a concept used liberally in other scenarios. Device identity and possible device integrity should be added to LOA.
4.3 Tokens	20	Recommend writing in the third person, entirely, and replacing "something you know, something you have, and something you are" with "something one knows, something one has, and something one is".

4.3 Tokens	21	"More generally, something you are does not generally constitute a secret. Accordingly, this recommendation does not permit the use of biometrics as a token." This spec forgets that the purpose of 800-63-2 is to have confidence in authentication, it's not about secrets. A biometric is a great subset of something one has, in that it's quite extreme to lose a finger, iris, or face and have it misappropriated by an imposter. Biometrics have other challenges, of course, but to dismiss them because they aren't secrets misses the point.
4.8	Calculating Overall Assurance Level	"The overall authentication assurance level is based on the low watermark of the assurance levels for each of the components of the architecture." This approach presupposes that the attacker has reasonably complete knowledge of all five aspects of how the system's authentication is constructed and has the wherewithal to attack at the most vulnerable point. Also, by combining the five separate levels into one number, it can lead to obscuring detail that might be useful in differing use cases that might have different thresholds.
5. Registration	Overall	Consider whether registration and issuance should be a separate specification. This is the lengthiest and least technical section. It also overlaps, for federal employees, as you point out, with other specifications. It also seems subject to rapid change as other means to identity proof become accepted, such as using social media.
5.3.1 General Requirements per Assurance Level	32	"At Level 2 and higher, the Applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other PII. Detailed level-by-level identity proofing requirements are stated in Table 3." The rigor here seems to be inconsistent with the vagueness allowed in Section 5.3 for pseudonymous credentials for Level 2.
6. Tokens	Overall	The scoring system does not allow for "extra credit" for multiple tokens of the same type. If one knows multiple passwords, PINs and knowledge-based answers, it certainly is worth more. Perhaps LOA needs more resolution since knowing multiple secrets may not qualify for the next level. The same holds with multiple tokens possessed.
8.1 Authentication Overview	69	"Further, detection of authentication transactions originating from an unexpected location or channel for a Claimant, or indicating use of an unexpected hardware or software configuration, may indicate increased risk levels and motivate additional confirmation of the Claimant’s identity." This abrogates the responsibility of this spec. LOA should cover everything related to confidence in the identity of the claimant, either within the spec, or by pointing to other specifications. I grant you it's entirely reasonable to not try to take on the wide range of environmental attributes that could be considered, such as claimant's login history in time and place and estimated location integrity. nevertheless, LOA should consider all factors in its computation.
8.1 Authentication Overview	70	You are forced to use the term "secondary authentication credential" to refer to the other definition of token, as SAML, for example, uses it. Please add it to the glossary and make a note to its dual definitions.

9.1 Assertions Overview	83-84	Please, please reconsider the use of "direct model" and "indirect model" when you describe what SAML Web SSO uses the term "artifact" for. And indeed, you yourself use the term "reference" for this concept (which I recommend). The reasons I ask this are: 1) Direct and indirect do not accurately describe what happens. The explanation does not even use the words direct and indirect. And yes, you could go back and add those words, but they clearly haven't been necessary heretofore. 2) The terms direct and ***in***direct suggest that there are two methods, but it turns out there is a third: "proxy". 3) Most important, and superseding the other two points, in many government communities, the terms direct and indirect authentication are used to describe whether the Claimant authenticates to the Relying Party itself or a Verifier / Portal (Figure 6) that intercepts all traffic between the Claimant and the RP (direct) and the indirect model of Figures 4 and 5 where each of the three parties can communicate with each other. The FICAM Roadmap, DoD JIE IdAM Portfolio and IC IAA documents all use "direct" as described here.
9 Assertions	Overall	This section should discuss the relative assurance of the three models and whether they are equally secure at each assurance level provided the mitigations are applied.
Topics of Interest		"Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?" Yes, Level of Confidence (LoC)for Subject attributes should be parallel to LOA (but definitely not part of LOA). The FICAM Access Control and Attribute Governance Tiger Team (ACAGTT) produced an Attribute Management Roadmap that provides a starting point for NIST to continue developing an LoC model and there is additional material not in the document that is available. Having LOA and LoCs for some number of attributes in a form that makes them easily combinable allows for easy arithmetic to decide what level of access or volume of data to grant a user.

United States Postal Service (USPS)

USPS comments to NST SP 800-63-2 center on two basic subject areas; broading the scope for additional LOAs, and expanding identity proofing to include KBA:

A. The need to broaden the scope for Levels of Authentication (LOA). At present there are 4 levels defined and these levels do not provide effective coverage or applicability to many business processes; there is specific interest for broader definitions at the lower end of the LOA spectrum.
    a. One suggestion is to separate the LOA for the token from the LOA for the identity assurance. Perhaps a new Level nomenclature that reflects different LOAs for authentication and identity (LOA 2/1 = Level 2 token / Level 1 identity assurance)?
    b. Another suggestion is to expand the LOA number to accommodate additional one or two LOAs
    c. Organizations conduct business with the general public and have e-authentication requirements that are greater than what is defined as Level 1, yet do not have an identity proofing requirement at the same time. Memorized secret tokens are by themselves not sufficient. The difficulty then is how to define an appropriate LOA according to 800-63-2 that aligns with the business requirement
    d. FIDO is establishing new directions for stronger token assurance without maintaining parallel requirements for identity vetting. There are other commercial technologies that offer similar capabilities although they may not necessarily be FIDO compliant. This is an excellent example where an appropriate 800-63-2 LOA definition could specify a token/assurance requirement that would be satisfied by a FIDO compliant token.
    e. Commercial applications are developing e-Auth models that don't necessarily fit within the four distinct LOA definitions, but many have interfaces with US government systems
B. If KBAs are recommended, then the document should outline remote identity proofing to utilize KBA services. Additional guidance will need to be provided by the publication

MorphoTrust USA

Confidential Notice

Certain information in this proposal is protected from disclosure to the public because it is a proprietary trade secret or confidential commercial or financial information of MorphoTrust USA, LLC or its affiliates (individually and collectively, "MorphoTrust USA" or "MorphoTrust").

MorphoTrust has endeavored to identify each page of its proposal that contains any such proprietary or confidential information with the legends "**COMPANY CONFIDENTIAL – Not for Public Disclosure**" or "PROPRIETARY" (or words of similar import) somewhere on the relevant page or pages of its proposal. MorphoTrust's proposal includes all exhibits and appendices thereto, as well as all extrinsic documents and materials that may be identified and incorporated therein by specific reference. MorphoTrust's proprietary information typically includes, but is not limited to, information related to proprietary security features and related designs, techniques and materials, formulas, manufacturing methods, business plans, pricing and other financial information, technology and product roadmaps, and customer lists and references. Subject to applicable law, such proprietary or confidential information may not be disclosed (pursuant to freedom of information legislation or otherwise), reproduced in whole or in part, or used for any purpose other than the recipient's evaluation of this proposal, without the prior written consent of an executive officer or the General Counsel of MorphoTrust USA, LLC.

Summary of Proprietary Rights

MorphoTrust USA, LLC ("MorphoTrust") is the sole owner of the proprietary rights to pre-existing biometric, authentication, and secure credentialing technology; results, prototypes and systems, including all restricted computer software, commercial computer software and the source code thereto, and/or other commercial items that have been developed solely at private expense and which are anticipated by MorphoTrust to support and be necessary for the use of the research, results, and pilot system. MorphoTrust shall retain sole and exclusive ownership of all right, title and interest, including all intellectual property rights, in and to all modifications, improvements, derivatives works and inventions made arising out of or related to MorphoTrust's advancement of its pre-existing technology in furtherance of its contract with the Government. Accordingly, MorphoTrust shall retain the sole and exclusive right to pursue patent protection for any and all such modifications, improvements, derivative works and Inventions.

Suggestions and comments on the categorization of vectors which should be included in new Electronic Authentication Guidelines and on the context for issuing guidelines

What is very right about 800-63-2

It's clear that 800-63-2 has been applied to different contexts than intended. Users of the Internet are fortunate that this has been the case.

Many of our current online systems for user authentication have ignored a hard problem to solve amongst the 800-63-2 guidelines - Identity Proofing. It has been impractical to replace the step of establishing a user's true identity during the registration process for an account because of two problems:

- Brick & Mortar, Human Identity Proofing doesn't scale for creating Internet Web Site accounts
- Technology for High-Assurance *Remote* Proofing has not yet existing, including the uptake of Identity Credentials and the authentication to tie that user to a pre-existing credential.

It has become extremely important to Internet security that 800-63r2 did include Identity Proofing in its guidance criteria, or it may have been overlooked worldwide which may have allowed the internet to further devolve without trusted users. Still, the proofing problem is not fully solved. New guidance must include a framework for how to incorporate identity proofing at Internet scale for when the problem is better solved.

Suggestion to Change the Context of Where the Guidance Applies

The Assumed Context of 800-63

The current guidance assumes granting of a credential to a Federal Employee who has already been hired – they are sponsored by a participating Federal Agency. They can be identity proofed at an office location near their place of business. Their use cases are a subset of those on the widespread Internet, and of course, there was the pre-existing choice of a common physical credential technology.

Moves to the Web and Entirely Online

The guidance that is clearly needed now should move to where all facets and functions of the process of granting a credential – from enrollment, verification, issuance, and management to credential usage – can be performed entirely within an online (remote) context. US Citizens as users of the Internet utilize service providers headquartered across the globe and hosted in locations often not even known by the service provider.

But Stays in the Context of Citizen Identity

While the model for providing Identity Trust should be applicable in many domains of identity, the NIST guidance can remain geared toward Government Employees AND (as a constitutional entity representing the Citizens of the United States) include specific guidance toward a framework for Citizen Identity.

The framework of how the Government Employee and Citizen models work, however, should be applicable in other domains of identity. And whether intended or not, it may well be picked up to be used in those other domains.

Suggested Model of Trust

Goals

- Score the responsibilities of an Identity Provider (IDP) equally along the axes that matter to the Consumer being authenticated and to the Relying Party (RP).
- Allow commercial services to evolve to meet market needs for shared services that meet your model of trust.
- Support the development of Open Standards for any of the pathways between the IDP and the RP and between the Consumer and their Chosen IDP
- Ensure the qualities of Security, Identity, Privacy, and a Consistent User of a RP's Service

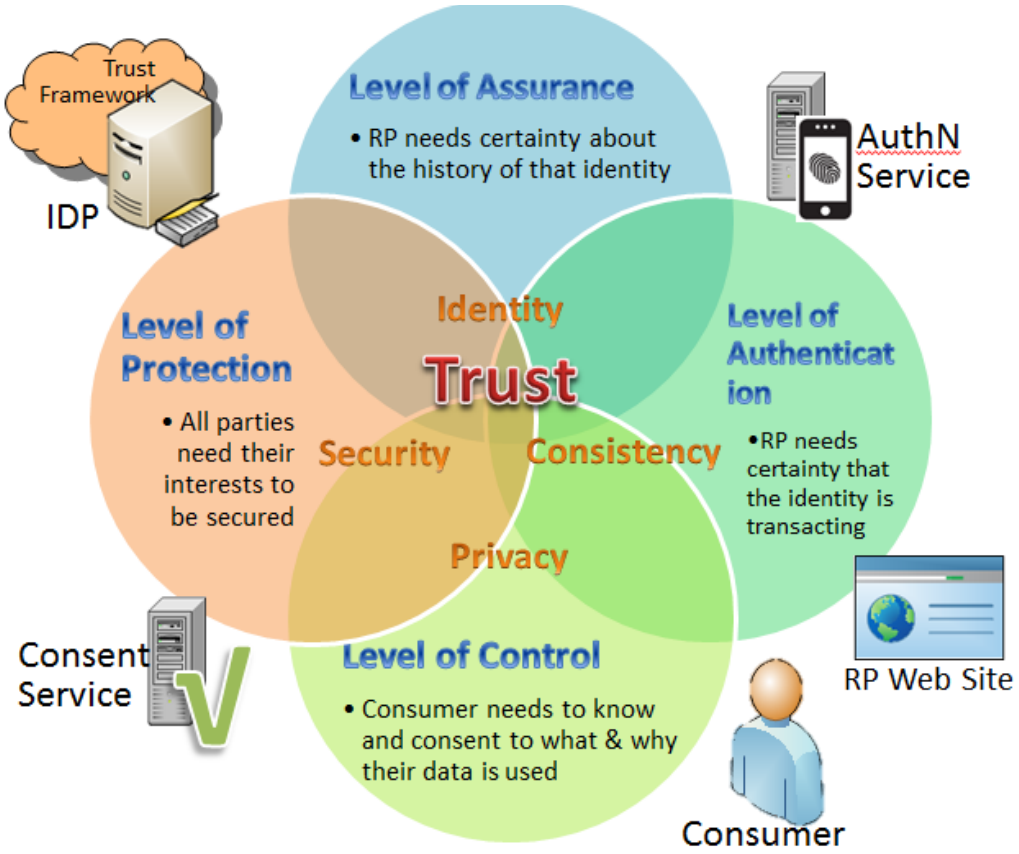


Figure 1: A Four Vector Model for calculating and assuring trust in Online Transactions

The Four Vectors that Constitute *Level of Trust*

Level of Assurance

MEASURES IDENTITY

Level of Assurance (which could also be called *Level of Establishment* in order to have LOE be a different acronym than LOA) is the measure of the certainty of the validity of the User to which the account is given. It can be measured before the account is granted (as in Identity Proofing) and then continually as the account is used (as in identity analytics for persistent vetting).

The valuation of "assurance" may be different within any particular realm of human identity – a scoring of the assurance of an account in a social setting may be based on usage and social contacts, but also include the degrees of separation from the Account Holder to another User they are interacting with. There are 8 realms of identity to consider, including legal, social, professional, etc.

Level of Protection

MEASURES SECURITY

Level of Protection measures the lengths to which security operations have made the end-to-end system impenetrable and the credential retain original validity. It is the domain of Cybersecurity expert evaluation.

Level of Authentication

MEASURES CONSISTENCY OF THE USER

Level of Authentication is the measure of confidence that the current User of the Service or Transaction is the original person to whom a credential was issued. This measure has been the focus of most Internet use cases so far, with mechanisms such as Touch ID from Apple introducing alternatives to passwords for authenticating users. This focus is largely because the repeated account creation process of self-attested attribute entry has been accepted as sufficient, even though the *Level of Assurance/Establishment* that services require is not met.

Level of Control

MEASURES PRIVACY

Adherence to privacy principles, obtaining consent, privacy policies, and consumer control of attributes are all measurable within *Level of Control*. It is a measure of the Consumer's protection, which could be trustmarked, measured, or assessed. In any environment where Consumer control is very low, Consumers may respond with their own protection measures of privacy – pseudonyms, deliberate error, etc. Returning control over identity to the Consumer will help increase accuracy as well as privacy.

An Example of Valuing Vectors Differently within a Particular Framework

Consider the example of a social network with an API ecosystem where Service Providers (e.g. Apps) in the ecosystem rely on the identity provided by one or more social account IDPs. Each particular Service Provider within the ecosystem may have different requirements in these 4 areas of Trust in their transaction.

A Shared Economy Service and its Users may have a specific mix of the 4 Levels above that truly matter to their interaction and the transaction. The Service Provider assesses their risk exposure for the transactions that they want to enable online. *Excluding* ability to pay, which is not an identity issue, and utilizing a None, Low, Medium, and High ranking system for simplicity, the mix may look something like the following:

- Low Level of Assurance/Establishment, based on a social-account scoring that indicates whether the account is new or fraudulent, and a reputation system
- Medium Level of Authentication, because the Shared Economy Service Provider needs to know that the assured account is not being reasonably used by another party
- Medium Level of Protection, because the credentials do not require high protection end-to-end
- High Level of Control, because Consumers truly do not want to be tracked utilizing a Shared Economy Service that can be anonymous, provided that reputation and payment keep the transaction solidly reliable and safe

Since these parties operate in a social framework, the scoring and valuation of items like Reputation and Social-Account Reality Score is the province of the Social Trust Framework provider. The Trust Measurement System should support their ability to provide scores that are meaningful to their parties.

Note on Ability to Pay

The level of risk in payment for a service and the absorption of that risk throughout the system are well covered in today's credit card transactions. It may, therefore, not be a scored item in the new NIST 800-63-2 guidance. It can be left to scoring of the credit and ACH providers.

Suggestions on "Levels" that Matter to RPs but can be understood by Consumers

Gradations

It is sensible to have four to five gradations publicly available to Service Providers and that the gradations are able to be understood and fulfilled by Consumers.

One or two additional levels of Security and Top-Secret security clearance should be available above and beyond the base gradations, but not typically publicly available for online interactions. For instance, an administrator may have to prove Security cleared Level of Trust in order to perform system-wide operations.

Naming

Naming of Levels of Trust must be understandable to the widest population of potential users. Naming could be left to the domain/framework in order to support flexible differences between calculation methods, particularly in the 8 domains of identity.

Capabilities for Add-On Layers on Top

The framework must provide for the extensibility of additional "Levels of Y" that may apply in a particular identity domain. Scoring another level and normalizing it into the calculation can be performed by the Framework Provider as an additional feature that they assure within their domain.

MorphoTrust Involvement

David Kelts, employed by MorphoTrust, has fully appreciated the opportunity to respond with content and would welcome the opportunity for MorphoTrust to be included in future discussions or review cycles of NIST 800-63 Guidance.

Experian

Experian appreciates the opportunity to provide comment and provide recommendations for consideration in the future versions of NIST SP 800-63. We have been very active in this space and provided previous recommendations which helped in the development of the current 800-63-2 guidelines. As one of the first certified IDPV's in this space, I believe we are in a unique position to provide insight based on our ongoing servicing of federal clients and seeing firsthand what works well and where we need improvement. Based on our experience to date, and the current and future needs of our clients, we have come up with the following:

General Comments

Recommendation: Allow for greater flexibility
Within the existing NIST SP 800-63-2 Guidelines for LOA2 and LOA3 Remote Identity Proofing, there are numerous references to government documentation and account information, and direction around how this information may be used for identity verification and credential issuance. While Experian interprets these referenced documents (e.g., Driver's License, Passport) and accounts (e.g., checking account, savings account, utility account, loan or credit card) and methods for verification to be suggested guidelines, many clients interpret these references as hard requirements. This creates a difficult situation for the IDPV's when the document and account examples referenced are not consistently available for the majority of the population. For example, we have found that driver's license information is only made available for verification across 30 or less states. This number continues to decrease as state level legislation increasingly restricts the access and use of this data. The passport reference is also problematic given the inability for private sector IDPV's to access this protected information. Experian recommends that further language be added to the guidelines, indicating that alternative forms of identity and account information may be used, assuming they are unique to an individual and have been verified through record checks either with the applicable agency or institution or through credit bureaus or similar databases. This will allow IDPV's to better utilize their ability to uniquely identity users within records while maintaining the intent of the applicable level of identity assurance. This will help to ensure that the right people are able to achieve the appropriate level of identity assurance (reducing false rejects) while continuing to prevent the wrong person from falsely obtaining a credential.

Recommendation: Allow for the use of emerging technologies
The existing 800-63 guidelines do not appear to contemplate the use of new technologies for identity verification and credential issuance. As an innovator in this space, Experian continues to invest in new technologies and services to better verify identities while anticipating future needs of our clients. Through the use of extensive data assets and new technologies, we have the ability to not only verify a user but also link the user to the devices used to access services. This approach allows us to establish a trusted relationship between people and things throughout the identity lifecycle. It is our opinion that this identity relationship management can further enhance the identity proofing process while offering an alternative approach to the current guidelines. For example, within the LOA3 guidelines an RA is required to verify the identity elements supplied by a user, including both a government ID number and account number, ensuring this information is linked to a user in records. There is a further requirement to confirm the ability of a user to receive a communication to either the physical or electronic address linked to a user in records. Through the use of identity proofing and device intelligence, Experian can take the identity verification process beyond simple identity element verification by associating financial

accounts to devices, utility accounts, biometrics and linking an electronic address to a device, ultimately enabling alternative ways to achieve the same level of confidence envisioned for LOA2/3 and 4. The request would be for NIST to be open to these new approaches and reference the potential consideration based on the RA's or IDPV's ability to substantiate or demonstrate how these alternatives meet or exceed the intent of the established guidelines.

Responses to questions below:
1. What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

2. Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

Answer: Identity Proofer, Token Manager (including device)

3. What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

Answer: As mentioned above, the use of device verification and intelligence allows for linkage of an identity to a preferred device. This could enable the recognition of a device as a token for ongoing verification. Adding a biometric registration capability to a verified device could allow for the remote registration of an LOA4 credential. This would significantly improve the overall consumer experience while enabling increased scalability for agencies currently forced to register in a face to face environment, all the while achieving the same or higher level of verification standards.

4. What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

Answer: From a consumer perspective, we hear that the requirement to provide financial account information for verification purposes is intrusive and not well received. From our perspective, the verification of a financial or utility account does little if anything when attempting to obtain identity assurance. The verification of identity elements with the use of risk scores and progressive KBA's, is much more effective at detecting fraud while establishing a higher level of confidence for a true consumer.

5. What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

Answer: Device Verification. The requirement for ongoing monitoring of an identity, re-proofing of an identity and reissuance of a credential, based on either an identity attribute change, new risk factors introduced (identity compromise), or time based at minimum.

6. Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

Answer: Not sure how this would be possible.

7. What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

Closing Remarks:

Based on our interaction with our federal clients, and our experience offering certified identity proofing solutions to government agencies, Experian believes that NIST SP 800-63-2 does not adequately reflect the current technology and data capabilities of identity proofing and credential service providers, while at the same time includes requirements that are either not broadly achievable or restrict providers from establishing better strategies and approaches to identity proofing. The current requirements often result in a very high false-rejection rate given the strict, unclear and somewhat outdated approach to establishing the appropriate level of identity assurance. In addition, the length of time between NIST publication updates makes it almost impossible for NIST to adequately reflect new technologies used for identity proofing within the published guidelines, while at the same time not offering the necessary flexibility in the language to allow for alternative strategies which achieve the same mutual goal of identity assurance.

This opportunity to provide feedback at an industry level is definitely a great step in the right direction. Further collaboration, either directly with the industry or, through framework providers (e.g. Kantara and others) on an ongoing basis will ensure that future publications take into account feedback from key stakeholders, encouraging further adoption of the subsequent releases. NIST will need to have the flexibility to respond to changes in technology and industry more rapidly in order to stay relevant. This continuous dialogue along with some mechanism to enable more rapid revisions will greatly assist everyone involved.

We look forward to continuing our active involvement in this dialogue.

Identity Management Subcommittee of the CIO Council's Privacy Committee

The following are high-level privacy considerations the Privacy Committee IDM Subcommittee recommends NIST consider in revising 800-63-2

- Explicit references to privacy and the role of the Senior Agency Official for Privacy within an agency should be addressed as well as the relationship between E-Authentication and privacy recognizing the sometimes competing privacy risks this can present (e.g., identity proofing needed to protect privacy but setting up a system can present additional privacy risks).
- Establishing Identity Management (IDM) systems are often handled by the Chief Information Officer organizations, given the expanding role and importance of the Senior Agency Official for Privacy, more privacy-specific guidance is needed in technical areas such as E-Authentication. Including references to the relationship between IT and SAOP organizations could better encourage such collaboration.
- The relationship between 800-53 Appendix J and 800-63-2 should be addressed and tie to the Improving Consumer Financial Transactions Executive Order.
- High level considerations for privacy should be built into this document specifically as they relate to implementation of fair information practice principles and in particular issues of redress (i.e., individuals unable to electronically authenticate because of erroneous data used in identity proofing processes, identity theft), consent (e.g., mechanisms for the individual to consent to use of their attributes for electronic authentication transactions in a way that is informative but enables federated approaches), minimization (e..g, using the minimum necessary to authenticate and not requiring a higher LOA when not necessary (though enabling choice to use a higher level credential for a lower LOA transaction) activity tracking (should limit use of authentication data for purposes unrelated to the authentication transaction) and notice (how does the individual know how his or her data is processed especially in a component identity services model). The FICAM/NSTIC privacy principles should be woven into 800-63-2.
- Address potential privacy act considerations in building electronic authentication transactions (in what set of circumstances could the Privacy Act be implicated, in which circumstances are they not.
- There is a need for common terminology between FICAM and NIST E-Authentication guideline. The lack of standardization makes it difficult for agencies (and especially privacy professionals that may not reside in IT organizations) to assess and evaluate solutions.
- Should address privacy responsibilities in a componentization model so that at the end of the day when agencies mix and match services they are still meeting all the privacy requirements.
- Recommendations on options available for Federal Agencies in identity proofing – guidelines on how to perform functions using agency-held data but explicitly recognize that authoritative sources of data may be restricted by law.
- Options for privacy enhancing technology models would be helpful for Privacy professionals. Recognizing that there are no privacy risk free options, some potential models explained with the privacy enhancing features explaining how they are privacy enhancing and any residual risks or new

risks presented by their implementation. For example an illustration of the broker model would be helpful.

- Currently 800-63-2 is scoped to individuals and is US person centric but there is a need for guidance on both how to electronically authenticate organizations as well as immigrant populations.
- Agencies (Relying Party in IDM terms) want to provide online services (e.g., recreation.gov, mySSA, myE-Verify, HHS, etc.); this requires a certain degree of confidence in the identity presented depending on the risks presented by the online application (see OMB M-04-04 on levels of assurance). To achieve the desired level of assurance, federal agencies often seek out electronic authentication solutions from a third-party Credential Service Provider (CSP).
- In the *remote* identity proofing process government agencies are typically astute at identity resolution (e.g., which Jane Doe among many Jane Does is this?) within their systems, however identity validation (e.g. is the information accurate?) and identity verification (e.g., is this really Jane Doe?) are considerably more challenging for agencies especially if they do not have an existing and/or longstanding relationship with the citizen/customer or access to authoritative data that would enable identity validation from an authoritative source. As a result, many government agencies (and in commercial sector) have turned to "data brokers" that use credit data (e.g., Experian, Equifax, etc.) to perform identity proofing functions through a mechanism called Knowledge Based Authentication (KBA). These data brokers use credit data to ask the claimant (citizen/customer) questions only he or she should know the answers to (e.g., which of the following addresses did you reside at? Which of the following is your loan amount from ABC financial institution?)
- Dynamic KBA solutions offered by data brokers have been widely adopted across the government for e-Authentication implementations, but there are significant challenges and unknowns because although the questions and answers are supposed to be based on information that is known only by the individual, it is unclear how true this assumption is. In addition, some demographic populations (e.g., immigrants, young adults) are unable to electronically authenticate in absence of a US credit footprint.
- Despite KBA challenges, alternatives to KBA through a data broker are not readily available to the federal government at this time and connecting to authoritative sources of data (often held by the federal government) may not be an option given authoritative source data purpose specifications and use limitations in law.
- Corroboration techniques used by data brokers for identity validation are not transparent to agencies and in absence of a KBA standard, agencies cannot evaluate whether the KBA solution meets the requisite level of assurance. KBA standards would be helpful for agencies to develop KBA solutions based on internal data.

Kantara Initiative Identity Assurance Work Group (IAWG)

Introduction
Kantara Initiative and its Identity Assurance Working Group (IAWG) welcome the opportunity to comment on NIST SP 800-63(-2). This document is one of the primary sources of the Kantara Identity Assurance Framework's Service Assessment Criteria, and members of the IAWG have studied and analyzed SP 800-63(-2) extensively for a number of years. Kantara Initiative's IAWG submits the included comments for the consideration of the NIST reviewers.

Kantara Initiative and the IAWG believe NIST SP 800-63(-2) is a mission criticaldocument that would benefit from a number of modifications to support the wider international and commercial adoption, beyond the original intended scope of use, for the benefit of trusted identity schemes. As NIST works through its assessment of responses to its SP 800-63(-2) Solicitation for Comments, Kantara Initiative's IAWG is ready to engage further, through industry facilitation and participation, in order to continue to assist in the revision and improvement of this important publication.

Context

Kantara Initiative is a membership organization that operates as a US 501 c6 to provide strategic vision and real world innovation for the digital identity transformation. Kantara Initiative enjoys the benefit of drawing upon the multi-disciplinary and international expertise of members including CA Technologies, Experian, ForgeRock, IEEE-SA, Internet Society, Nomura Research Institute (NRI), Radiant Logic, and SecureKey.

Kantara Initiative connects a global, open, and transparent leadership community of identity services and systems experts through our initiatives including the: Identity Assurance Framework2, Identity Relationship Management3, User Managed Access4, Identities of Things5, and the Minimum Viable Consent Receipt6.

Further, Kantara Initiative operates as the premier US Trust Framework provider for the US Identity Credential and Access Management (ICAM) program under the General Services Administration (GSA). The Kantara Initiative Identity Assurance Program, operating on the behalf of the ICAM, provides an instantiation of Trust Framework verification (through ICAM) and operations (through Connect.gov) to prove the benefits and efficiencies of interoperability of trusted identity services technology and policy layers.

2 https://kantarainitiative.org/confluence/x/e4R7Ag
3 https://kantarainitiative.org/groups/irm/
4 https://kantarainitiative.org/groups/user-managed-access-work-group/
5 https://kantarainitiative.org/groups/idot/
6 https://kantarainitiative.org/groups/ciswg/

General Recommendations
Recommendation: Tighten Requirements Language

Consider the guidance in ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards,* Annex H, which provides requirements for the structure and drafting of international standards. This document is a valuable reference for authors of standards who wish to convey information in a clear, concise and consistent manner. This ISO document provides for the expression of provisions in the following manner: We recommend that NIST adopt this syntax for expressing provisions in a future SP 800-63(-2), and indeed, as a general policy, in all future revisions of all NIST publications.

INDICATION	EXPLANATION
Requirement	the terms "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted
Recommendation	the terms "should" and "should not" indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited
Permission	the term "may" and "need not" indicates a course of action permissible within the limits of the document
Possibility	the term "can" and "cannot" indicates a possibility of something occurring

NIST SP 800-63(-2) uses inconsistent language to describe its content with the result for potential ambiguity and misunderstanding by the reader. For example, Table 3 contains identity-proofing requirements, but the syntax is a mixture of sentence fragments, narrative descriptions of procedures. This table is the foundation for evaluating identity proofing implementations and the current lack of clarity results in inconsistent implementations. The titling of the document as 'Guidelines' is in conflict with the intended mandatory adherence to its provisions. We recommend that NIST adopt syntax similar to ISO or consistent with IETF RFC 21197 for expressing requirements using the verbs *"SHALL"* and *"SHALL NOT."* It is noted that there are only a few formally expressed *"SHALL"* type requirements.

Initially, NIST may consider clarifying the rows labeled "basis for issuing credential." It seems clear from context, but nowhere is it stated, that the contents of that row express criteria that must be met prior to issuance of the credential. Stating the contents of this row clearly as requirements, e.g. "applicant shall provide a valid, current government identity document," allows the reader to understand what behavior is required and by whom.

7 https://www.ietf.org/rfc/rfc2119.txt

Recommendation: Increase Flexibility

Consider following an approach similar to Common Criteria8, in which a generalized requirement syntax supports the creation of Security Target and Protection Profile documents which are used specify the requirements that implementations must follow.

It is acknowledged that Common Criteria is applicable to evaluation of products, and not services, but the concept of defining requirements and then using such defined

requirements to describe the capabilities of services can support more flexibility in the expression of requirements.

Consider application of this conceptual approach to NIST SP 800-63(-2) by restructuring the document to first define the syntax and terminology of identity assurance requirements in the areas of identity proofing, token management, credential management, etc.; and then to use that terminology to define Assurance Profiles that contain logically grouped sets of requirements. This permits the expression of OMB M-04-04 assurance levels as well as other sets of requirements developed for myriad Purposes.

8 https://www.commoncriteriaportal.org/

Responses to NIST's Questions

O *NIST1: What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?*

> *What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction?*
>
> The US FICAM approach based on NIST 800-63(-2) has been reasonably effective to provide an initial program based upon the Trust Framework Model. In this program the US Government is the Trust Framework Authority where approved industry organizations are responsible for the governance and execution of verification of policy practices and deployment of technical profiles. The UK IDAP provides a similar program. In the near future the European Commission will publish an interoperability framework for the consideration of European Union Members in the form of the eIDAS9. Note that each EU Member will have variance in their approach to implementing EC Directives, although they will all meet the baseline requirements of the applicable Directive.
>
> *How is interoperability of divergent identity solutions facilitated?*
>
> The term "identity solutions" is broad in nature. At the minimum it is suggested that interoperability is seen in terms of at least the following components as unique and distinct services:
>
> - o Token Manager
> - o Identity Proofer
> - o Credential Manager
> - o Identity Registrar

O *NIST2: Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?*

Token Manager, Identity Proofer, Credential Manager, Identity Registrar

O *NIST3: What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.*

9 https://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyonicam

Recommendation: Add consideration of resilience to remote identity proofing

Incorporate NIST IR 7817 concepts of reliability and resilience to the model. Define requirements for identity proofers to notify credential issuers when information has been discovered as breached, and processes for resolving and adjudicating remote identity theft. However, this approach may provide difficult to adopt due to the privacy implications of sharing identity compromise information with CSPs.

Recommendation: Identify remote identity proofing for risk-tailoring by RPs

Consider using the aforementioned profile approach to support scenarios that do not permit remote identity proofing. For example, relying parties that are government services pertaining to spousal conflict should be able to avoid the risk that spousal relationships could enable remote identity theft.

Recommendation: Clarify the use of Privacy Impact Assessments

Consider reference to requirements, likely external to NIST 800-63(-2), for the performance of a Privacy Impact Assessment on the overall credential lifecycle, identifying the points in the process when PII is created, gathered, shared, transferred, destroyed, or archived.

Recommendation: Clarify the requirements for address of record

NIST SP 800-63(-2) defines the address of record as a residential address (p. 6) and provides distinct requirements for verification of address of record versus other contact information such as telephone or e-mail address. Please clarify the requirements for verification of residential address and for verification of communications addresses during identity proofing.
We recommend maintaining the distinction between residential address of record and (postal) communications addresses, because of the differing risk mitigation characteristics of the verification processes. Verification of residential address imposes a reasonable degree of legal accountability upon the subscriber. On the other hand, verification of a communications address ensures that notifications can reach the subscriber.

O *NIST4:* W*hat privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?*

Recommendation: Address privacy risks through user-centric risk Assessment

As a consequence of being driven by a system-centric risk assessment, NIST 800-63(-2) does not sufficiently address the privacy concerns of users. In general, NIST 800-63(-2) does not address core privacy principals identified by
NSTIC and does not address privacy as it relates to selection of attributes to present to the world, e.g. a persona.

For example, *Alice* operating as a private citizen (G2C) and accessing a government service has different privacy expectations than *Alice*, acting as an employee of *FooEnterprise* and accessing a government system as part of a work assignment, or perhaps as a government employee herself, involved in the provision of that service.

Requirements to address privacy concerns are often not a "one size does fits all" prospect. Definition of privacy requirements and inclusion in certain profiles will enable identity services that meet a broader range of privacy needs. It's also worth noting that the ICAM TFPAP has recently added some privacy considerations to the ICAM scheme.

Recommendation: Privacy Terms

Consider incorporation the following privacy terms in the updated model, with appropriate entitlements according to Assurance Level:

- **anonymity**: the property of a service of not disclosing identifying information about users
- **pseudonymity**: the property of a service that permits users to identify themselves by aliases and other unverified names
- **reversible pseudonymity**: the property of a service that performs identity proofing during registration but permits users to identify themselves by aliases and other unverified names. Identified authorities are permitted to obtain the verified name of the user under controlled circumstances
- **unlinkability**: the property of a service that prevents disclosure of multiple accesses of a service or resource by the same user.

O *NIST5: What requirements, processes, standards, or technologies are currently excluded from 800-63(-2) that should be considered for future inclusion?*

Recommendation: Electronic Authentication and Identification

Expand the scope to Electronic Authentication and Identification, reflecting the functional linkage of those two security mechanisms. The result of the process is not just a yes/no decision whether the claimant is who they say they are, it is also

the delivery of an identification of the subscriber to the relying party. That identification could include their name, or a pseudonym, or an opaque identifier. The entire process from unknown claimant to identified user is frequently called "authentication and identification" rather than solely authentication.

Recommendation: Note that "subject" and "subscriber" are synonyms in related specifications (e.g. X.509 vs. 800-63(-2))

Recommendation: "Identity" should become "Identifier"
We recommend considering use of the term "identifier" to mean "a set of attributes that uniquely describe a person within a given context." To support the case when such an identifier is also a single attribute (e.g. a UID, national ID number, etc), consider potential use of the term "unique identifier" to uniquely describe a person within a given population and potentially within a given context.

Recommendation: Define "Context"
Context is used in the definition of identity/identifier, please define or remove from the definition. Section 5.3.1 states that "all privacy requirements shall be satisfied", and it is recommend that NIST consider clarification with regard to which privacy requirements are intended to be satisfied.

Recommendation: Identity Register
Consider adding to the model, the concept of an Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that are inherent to this role, including the protection of registration data for future dispute resolution balanced with the user risk-mitigation goal toward minimizing instances of PII generation. The Identity Register may provide support for federated authentication, identification, credential reliability, and recovery services.

Recommendation: Elevate Biometrics
It is recommended that "Biometrics" should be included as a section in the document alongside "Identity Proofing" and "Tokens." At high levels of identity assurance there is certainly a role for each of these different aspects of authentication and identification. Each aspect answers the standard authentication and identification questions such as: something you know (shared secret), something you have (token), and something you are (biometric).

Recommendation: Inclusion of next-generation multi-factor authentication
Consider expansion of the scope of use for two-factor credentials to include technologies such as asymmetric cryptographic device authentication that employs challenge and response for second factors.

Recommendation: Address Liability through industry engagement
In general, Trust Framework Providers have not yet addressed the liability model for federated credentials, and NIST 800-63(-2) does not address the topic at all. Technology does not stand in the way of expanding credential re-use, so much

as do the concerns with permissible technology use potential liabilities. Is the Credential Service Provider liable for damage done with a compromised credential, and if so, under which circumstances? PKI and the CP are the only largely deployed trust frameworks that address risks and limitations. It is recommended that an effort should be considered within NIST, or other appropriate channels, to address liability with regard to recovery of damages and the limitations of risk for the CSP.

Recommendation: Decouple Identity Binding
Permit identity proofing to occur after token issuance.

O *NIST6: Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?*

Recommendation: Support definition of Risk Confidence Factors in addition to the four-levels mode
Instead of grouping assurance profiles solely as 1,2,3,4 per OMB M-04-04 requirements, permit the expression of risk confidence score with multiple factors including identity proofing, token strength, multiple factors, biometric verification, etc.

NIST may also consider the introduction of risk confidence factors to re-define, or inform, the Assurance Levels. This approach may be considered in terms of how a new "X"-63 may be structured.

O *NIST7: What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.*

Kantara Initiative does not have supporting data to comment on this topic. However, some consideration may be given to the implications of identity context including such varying attributes as behavior, time, and location for example. As the role and implications of identity context becomes more visible it is possible that identity context will play a role in the elevation of trust on a transactional basis.

NIST may consider "trust elevation" as a developing field of study. Further the general recommendations regarding further definition of requirements and possible modeling of Common Criteria may enable a more flexible framework to enable outcome based approaches to the measurement of assurance in real time as transactional and based upon particular trust components.

Daon

These comments relate primarily to the role of biometrics in e-authentication and are meant to address your 5th topic of interest:

- What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

However, there are some more general comments included at the end.

Continued on next page.

By	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment [1]	Comments	Proposed change
Daon-1		2	3rd full para on pg 3	te	Biometrics are not considered authentication tokens because they are not secrets; however, they may be used to activate other secret-based tokens. Therefore, they may be used in Multi-factor Tokens (as defined in 6.1.1) but not in Multi-token authentication (as defined in 6.1.2). This addresses their use in "serial" verification, through local activation, but not "parallel" verification where the second factor is verified at the verifier. This document should allow for the use of biometrics in the second case where: a) The biometric is used as a 2nd (or 3rd) factor only, and b) The biometric is protected during transmission to the verifier. For example, a Single-factor crypto token uses a locally stored key within a cryptographic protocol (e.g., TLS), achieving LoA2. When a biometric is added to activate that key, it becomes a Multi-factor crypto token, achieving LoA3. However, if the Single-factor crypto token is both verified and used to create a secure channel to the verifier, the biometric may be transmitted over that secure channel and verified at the verifier rather than locally. This is not	Add to the end of this paragraph: "However, biometrics are included in the list of defined token types for use as a second or third authentication factor only." NOTE: Other changes below relate to this same comment (Daon1-16).

					currently supported.	
Daon-2		2	1st para on pg 4	te	Rather than disallow biometrics as a token type, restrict them to use as a 2nd or 3rd factor given the conditions cited above.	Change 1st sentence to read: "Biometric characteristics do not constitute secrets suitable for use as a single authentication factor." Change 3rd sentence to read: This document supports the use of biometrics to "unlock" conventional authentication tokens, as a 2nd or 3rd factor in multi-token authentication, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process. OR Delete entire paragraph.
Daon-3		3	Biometrics entry, 2nd para	te	Same as above.	Change 2nd sentence to read: "In this document, biometrics may be used to unlock authentication tokens, as a 2nd or 3rd factor in multi-token authentication, and prevent

						repudiation of registration.
Daon-4		4.3	4th para on pg 21	te	Same as above.	Add to last sentence: "except when used as a 2nd or 3rd factor in multi-token authentication."
Daon-5		4.3	5th para on pg 21	te	Same as above.	Replace last 2 sentence with: "If a single factor is presented to the Verifier, it must contain a secret. Additional factors used to protect (activate) the secret token do not themselves need to be secrets. If multiple factors are presented to the Verifier, at least one must contain a secret and others must be adequately protected."
Daon-6		4.3	2nd para on pg 22	te	Same as above.	Add 3rd paragraph (between current 2nd & 3rd), reading: "In addition, biometrics may be used as a 2nd or 3rd factor in a multi-token authentication. For example, consider again the piece of hardware (a token) which contains a cryptographic key (the token secret).

						The cryptographic key produces an output (the token authenticator) which is used in the authentication process to authenticate the Claimant and to establish a secure channel to the piece of hardware. The biometric may then be captured on this hardware, transmitted over the secure channel, and authenticated at the Verifier. In this case, an impostor must steal the encrypted key (by stealing the hardware) and replicate the fingerprint to be successfully authenticated, just as above. This specification considers such a device to effectively provide two factor authentication, since both the secret and the biometric are required to complete the authentication.
Daon-7		6.1	1st para	te	Same as above.	Change 1st sentence to read: "In the e-authentication context, a primary

						token contains a secret to be used in authentication processes." Add before last sentence: "Secondary tokens (those used as a 2nd or 3rd factor) may not be secrets (i.e., may be *something you are*).
Daon-8		6.1.2		te	Same as above.	Add 10th bullet: • *Biometric Token*. A sample of a biometric characteristic captured from the claimant. A reference sample is collected during registration and stored within the CSP. During authentication, the claimant presents their biometric characteristic to a biometric reader which captures a fresh biometric sample which is securely transmitted to the verifier where it is matched to the reference sample to determine if the two samples originate from

						the same human being. Biometric tokens may only be used as a 2nd or 3rd factor in multi-token authentication; they may not be used alone as a single-token. Biometrics are *something you are.*
Daon-9		6.2	Table 4	te	Add biometric threat examples.	Under Duplication, add the following example: A biometric sample is copied to create an artefact.
Daon-10		6.2.1	Table 5	te	Add biometric threat mitigation.	Under Duplication, add the following mitigation: - Use biometrics which are more difficult to discover (e.g., those not publicly exposed) and/or incorporate biometric liveness detection mechanisms, including challenge/response.
Daon-11		6.3.1.1	Para 1	te	Add note regarding biometrics.	After 1st para, add 2nd para to read: "Although biometric tokens may not be used in single-token authentication, the

						associated token and verifier requirements are included in Table 6 in order to specify their requirements when used in multi-token authentication."
Daon-12		6.3.1.1	Table 6	te	Add biometric token requirements. NOTE: Accuracy proposed is taken from NIST SP800-76-2.	Add row at end of table with the following entries: Token Type: Biometric Token Level: N/A (used only as 2nd or 3rd factor) Token Requirements: Biometric tokens shall be encrypted during storage and transmission. Verifier Requirements: The verifier shall implement a biometric matcher capable of achieving an FNMR less than or equal to 0.01 at an FMR of 0.01 (with one or more samples).
Daon-13		6.3.1.2	Table 7	te	Add biometrics to Table 7 to indicate their use in multi-token authentication.	Add last row as shown below: Biometric Token X X X X X X X Add last column as shown below:

						<table><tr><td>Biometric Token</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 3</td></tr><tr><td>Level 4</td></tr><tr><td>Level 4</td></tr><tr><td>X</td></tr></table> Where the row/column headers are unchanged other than the addition of rows/columns for Biometric Token.
Daon-14		6.3.1.2	1st para on pg 56	te	Rather than disallow biometrics as a token type, restrict them to use as a 2nd or 3rd factor given the conditions cited in Daon-1.	Change to read: The principles used in generating Table 7 are as follows. Level 3 can be achieved using two tokens rated at Level 2 that represent two different factors of authentication. Since this specification does not address the use of biometrics as a stand-alone token for remote authentication, achieving Level 3 can occur by either adding a Biometric Token (*something you are*) to a separate Level 2 token (either *something you have* or *something you know*) or by combining two separate Level 2 tokens from the *something you have* and *something you know* categories. Token (Level 2,

						something you have) + Token (Level 2, *something you know*) → Token (Level 3) or Token (Level 2, *something you have or something you know*) + Biometric Token (*something you are*) → Token (Level 3)
Daon-15		6.3.1.2	3rd para on pg 56	te	Same as above.	Add new paragraph between existing 3rd & 4th paragraphs: "Likewise, a Biometric Token may be combined with a Memorized Secret Token (*something you know*) or a Single-Factor Cryptographic Device (*something you have*) to elevate the trust of the Level 2 single-factor token to a Level 3 multi-token (and multi-factor) authentication."
Daon-16		7.3.1.3	First bullet	te	Biometrics should be protected to the same level as shared secrets.	Change first paragraph to read: *Credential storage* – Files of long-term shared secrets or biometrics used by CSPs or Verifiers at Level 3 shall be protected by access controls

						that limit access to administrators and only to those applications that require access. Such ~~shared secret~~ files shall be encrypted so that:
Daon-17		5.3.1	& Table 3	te	800-63 provides for remote identity proofing. However, although not stated, it appears that that the document as a whole, and the identity proofing requirements specifically, assume that the applicant is an adult. However, we have encountered situations where an agency applies 800-63 to children (i.e., 12 and older). Children typically cannot meet the requirements specified. Further, though KBA is not called out as a remote identity proofing method specifically, verification of data "through record checks either with the applicable agency or institution or through credit bureaus or similar databases" is cited and KBA methods have been found acceptable. Again, children are generally not able to successfully pass such checks. In fact, there is a significant portion of the population that cannot.	Specify alternatives (preferably not limited to in-person proofing) for identity proofing of children. Also, and as a minimum, clarify applicability of the SP so that it is not as likely to be incorrectly applied. NOTE: More specificity is required regarding the use of records checks and KBA as part of remote identity proofing, including performance metrics as applicable.
Daon-18				ge	Document should be updated to accommodate mobile devices, particularly with respect to browser references.	Left to NIST.
Daon-19				ge	Though developed for federal applications, SP800-63 has also been applied in other contexts, including commercial contexts. However, not all requirements	Consider identifying requirements that are "federal only" or issuing a

					in 800-63 align well with commercial needs and practices.	commercial version of SP800-63
Daon-20				te	As written, SP800-63 is overly restrictive and not innovation friendly. This inhibits adoption of newer technologies and solutions and limits you to "more of the same".	Consider making SP800-63 more 'risk-based', allowing for equivalent/comparable implementations and compensating controls, based on comparison of relative risks.
Daon-21				te	SP800-63 does not address trust elevation scenarios, but only zero-to-LoA(x) situations.	Consider requirements for "delta-authentications" where the subscriber has already authenticated at one LoA and then <within the same session and time window> initiates a transaction at a higher LoA.
Daon-22		multiple		te	FIPS140-2 is required for all cryptography; however, this does not address the situation in non-federal employee browsers and mobile OSs. Although the top products are all FIPS140-2 certified, when new versions are released, there is a lag time to their re-certification. Technically, this would violate the requirement. Although not critical for federal employees, this could be problematic for government-to-citizen applications. [Related to this, FIPS 140-2 certification is for a crypto module running on a specific	It is recommended that this situation be addressed.

					dot release of an OS on specific hardware, even to the chipset level. This can be problematic for an Android environment, for example.] Note: There are no certification requirements for any other authentication method. So an LoA2 password requires no certification while an LoA2 single-factor software crypto token (e.g., as implemented within a mobile/browser-based TLS protocol) does. Does this make sense?	

Crossmatch 1

Section	Subsection	Problem	Proposed Change
Executive Summary	Level 1	Document does not describe what Level 1 is good for, unlike Levels 2-4.	Level 1 should only be used to locally access applications that do not have a significant risk to the government or its citizens if authentication is compromised.
Executive Summary	Level 4	Document requires that only hard cryptographic tokens are allowed.	Allow cryptographic tokens to be stored on a secure server. Other mechanisms for proving physical ownership of a token should be allowed, given that those credentials are resilient from being copied. The system already relies on elements hosted by the secure server in order for authentication to function (notably certificate chains). There should be no appreciable loss of security by allowing tokens to exist in a FIPS 140-2 Level 2 hosted server.
Introduction	Paragraph about Tokens that are difficult to forge	The concept of token containing a secret should be removed from the document, allowing a richer and more usable authentication context. Biometrics should not be excluded because they are “weak” or “difficult to quantify”. Biometrics are a proven authentication	Remove paragraph.

		technology adopted on a broad scale for a number of applications.	
Introduction	Paragraph about Biometrics	While Biometrics are clearly not secrets, they can be used as tokens in an authentication framework. The positive security characteristics of biometrics for authentication should be reflected in a redefinition of token for eauthentication.	Remove the overly prescriptive token contains a secret perspective throughout the document.
Definition	Biometrics	Recognition is a very loaded term. The definition should be replaced – especially for the intended use cases of this document. Remove the note about how biometrics may be used (not applicable to a definition).	Automated Verification of individuals based on their behavioral and/or biological characteristics.
E-Authentication Model	Overview	The definition of token (contains a secret) is too prescriptive for many effective authentication use cases. Specifically biometrics is an effective authentication technology, and should have some location within a token framework.	Remove the overly prescriptive token contains a secret perspective throughout the document. While biometrics is not a zerorisk technology, with known issues of liveness and aging, they are not inherently more risky than the use of PIV cards controlled by a 6 digit pin. They deserve a place within an e-authentication framework, larger than just the role of mitigating a risk of

			incorrect credential issuance.
E-Authentication Model	Overview	Usability is a critical aspect of successful Authentication, but it is not mentioned. Unusable systems are often systems that are not adopted or are worked around, lowering effective security.	A paragraph highlighting the importance of usability should be inserted. The paragraph should highlight aspects especially for verification/authentication processes, but could also mention registration and credentialing. Perhaps a call for contributions or internal work can be devoted to fleshing this out.
Registration	Overview	Biometrics can and should be utilized for registration processes. The use of biometrics to help improve the trust of registrants, and to remove duplicate registrants, is well known, and should be mentioned in the document, as well as have a place in the level hierarchy.	A paragraph about applicants undergoing background checks should be added, as well as the use of biometrics to perform duplicate enrollment checks.
Registration	Threats	Add duplicate enrollment as a registration activity threat.	Add biometrics as a mitigation strategy towards that threat. Add this capability to Level 4 requirements for registration.
Registration	Issuance Mitigation Strategy	While biometric verification is mentioned in page 36 for card issuance, the table on page 30 for Unauthorized issuance does not mention the use of the biometrics on the PIV card that are collected for its current purpose.	Highlight biometric verification as part of mitigation strategy for Unauthorized issuance.

Tokens	Overview	Token should not be so prescriptively defined as containing a secret.	Allow tokens to not necessarily contain a secret, but also to refer to a secret stored elsewhere in the architecture.

United States Department of Agriculture (USDA) ICAM

Subject: Remote Identity Proofing at LOA 2 and LOA 3
Document Location: Table 3 on page labeled as 33
Comment: Need clarification on the verification of Government ID number and/or financial account number for remote identity proofing. Is it a requirement that the RA collect the Government ID number and/or financial account number from the Applicant and do an exact match of those numbers against Government and financial records to verify that there is a match? Or, can the financial account number requirement be met by verifying knowledge of recent account activity? Is NIST using the [3]financial account number[2] and [3]Government ID number[2] as a key to get to the actual data that needs to be validated (First Name, Last Name and DOB)? In other words, is the intent to validate the ID/account number itself, or to validate the information that is associated with that ID/account number?

Subject: Requirement for Address Confirmation
Document Location: Table 3 on pages labeled as 33 & 34
Comment: If the credential has already been issued at a lower level of assurance (e.g. Level 1), and the applicant is now being remotely identity proofed for a higher level of assurance e.g. Level 2), what are the requirements for Address Confirmation? The user already has control of the credential at Level 1. Does the Applicant need to prove the ability to receive physical or electronic messages at an address in their records before they can use the credential at Level 2 assurance?

For remote identity proofing for LOA 3, if the email address and physical address provided by the user cannot be verified as a linked pair in records, is the only option to send a message to the physical address? This introduces time delays for the Applicant to use their credential, and adds significant overhead to the remote identity proofing process. Are there alternatives that can be added so that send mail through the USPS is not required?

Subject: International (non-US citizens) identity proofing process
Document Location: Table 3 on pages labeled as 33 & 34
Comment: Agencies can determine what constitutes a valid Government issued ID as required, however Government IDs from outside of the United States are difficult to verify remotely due to international privacy laws. More guidance is needed for remote identity proofing of foreign nationals at LOA 2 and LOA 3 so that it can be done consistently across the Federal Government.

Veterans Affairs (VA) IAM

Part 1: General Comments

Recommendation: Include guidance regarding ID proofing above LoA1 for populations who don't have U.S. government issued photo IDs or an address of record.

This includes the homeless population and other populations who do not have or cannot get, for whatever reason, a U.S. government issued id.
Issue: The VA issues credentials at LoA2 for Veterans, but we are unable to issue these credentials to homeless Veterans because we are unable to meet the LoA2 criteria for ID proofing. In general, the homeless population has neither an address of record nor a U.S. government issued ID.
Include in NIST 800-63: Include additional/alternative procedures and identifiers that can be used for identity proofing at greater than LoA1 for people without a U.S. government issued ID. Some possibilities include:

- Trust elevation mechanisms and processes, such as:
  - Use of biometrics
  - Use of context specific data
  - Knowledge-based questions from closed sources
- Commercial two-factor authentication tokens, such as:
  - Google authenticator
  - Fast Identity Online (FIDO) compliant tokens
  - SMS messages sent to a registered mobile phone or email account
- Possibly the use of derived credentials. (Harmonize NIST SP 800-63 with NIST SP 800-157)

Recommendation: Include guidance on the use of foreign IDs in identity proofing

Currently SP 800-63 provides no guidance regarding the use of foreign credentials in the identity proofing process, leaving it up to individual agencies.

Issue: VA has veterans and service connected foreign nationals living overseas who need electronic access to their health information. VA needs to be able to provide authentication credentials at the LOA2, and possibly LOA3, level.

Include in NIST 800-63: Include additional guidance/mechanisms that will allow for the equivalent of LOA2-3 identity proofing when the only identity documentation is issued by a foreign government.

Recommendation: Implement an overlay/tailoring capability

We suggest implementing an overlay/tailoring capability similar to SP 800-53. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. We understand that an overlay can be dangerous in that it could dilute an LOA if inappropriate substitutions are made. But if changes are made that are comparable to LOA requirements, that would likely be a great benefit to communities that have different needs. It would also likely provide greater flexibility during the lifespan of a specific 800-63

version (i.e., communities won't need to wait for a new 800-63 version to implement an alternative approach that would be deemed satisfactory/acceptable at that point in time).

Recommendation: Add guidance on the use of Trust Frameworks and the communication between federal and non-federal trust frameworks:

Issue guidance regarding the establishment and use of Trust Frameworks to guide interaction and cooperation amongst public and private security domains. The policy should define the core elements of a Trust Framework including but not limited to legal, operational, and technical specification. Trust Frameworks are essential to ensuring the necessary level of security, privacy, information sharing, as well as proper technical interoperability. It also ensures all parties have a full understanding of all applicable obligations, responsibilities, accountability, and liabilities.

Acknowledge, address, and harmonize guidance with existing FICAM Trust Framework Solutions initiative.

Recommendation: Credential renewal guidance

Provide guidance that simplifies the credential renewal process and allows for the persistence of identity and use of a recently expired credential in obtaining a new credential of the same type.

Recommendation: Tighten requirements language

NIST SP 800-63-2 uses inconsistent language to describe its content, resulting in potential ambiguity and misunderstanding by the implementer. For example, Table 3 contains identity proofing requirements, but the syntax is a mixture of sentence fragments, narrative descriptions of procedures, and a few properly expressed “shall” type requirements. This table is the foundation for evaluating identity proofing implementations, and the current lack of clarity results in inconsistent implementations.

Recommend modeling the language used after ISO/IEC Directives Part 2. This document provides requirements for the structure and drafting of international standards and is a valuable reference for authors of standards who wish to convey information in a clear and consistent manner. It categorizes the expressions that can be found in a standards document into three types: statements, recommendations, and requirements. The definitions of these terms is useful to consider:

- A statement merely conveys information,
- A recommendation indicates that one among various options may be preferred or more suitable under certain circumstances,
- A requirement is an expression containing criteria that must be fulfilled if compliance with the document is to be claimed.

Requirements are expressed using the verbs *shall* and *shall not*. We recommend that NIST adopt a similar syntax for expressing requirements.

Recommendation: Enrich LOAs

- **The Problem:**
  1) The private sector is trying to use the 800-63-2 LOA structure and it’s not working. The NIST Guideline is too rigid and government-centric for private sector adoption and is not user-friendly in its current configuration. The consumer-centric market is rapidly being transformed into a relational digital enterprise of the Internet of Things. The NIST Guideline needs to re-purpose its focus on end user identity [and privacy control]. Note: This has a direct influence on controlling

privacy (as defined by access control, who has what privileges? When? Under what conditions or event?).

2) LOA 1 is quickly being eroded as social media private sector institutions and governments at all levels abandon the user-name and password as an access function due to escalating cybersecurity and identity threats and breaches.
3) The healthcare community is chipping away at LOA 2, as seen by the fact that the HIMSS Identity Management task Force recently endorsed LOA 3 for access to healthcare portals. See http://www.himss.org/files/HIMSS_IDMTF_IAPP_Recommendation_Final.pdf.

- **NIST Action**
  1) NIST needs to enrich LOA's 2, 3, 4 by adding functionality layers to their core components, e.g., via an attribute ecosystem. LOA 2, 2.1, 2.2 … 3.5, 4.5, etc., each with supporting trust marks. For LOA 3, everybody has to adhere to core components, and then to each desired level of add-ons. NIST has to define what these should be.
  2) NIST should convene groups to decide on a set of pre-approved devices for biometric devices, iris scans, etc., that would represent functionality levels for the three LOA classes and unique to Level 4, the acceptance of e-notarization where several states are in play with more to follow. NIST would determine the device mix.
  3) NIST needs to enrich the existing government LOA platform and process, by enriching digital identities and associated attributes. This would establish a digital marketplace for authenticated identities. The private sector could then adopt this enriched infrastructure for a quasi-seamless interface between government and the private sector, and within the private sector.

Recommendation: Address the following identified gaps in the existing document:

- Look closely at the LOA descriptions and ensure that "valid credential," "validate," "verified credential" and "verification" are well defined. Also describe the process required to "validate" verses "verify" a credential.
- Define "control of" and "possession of" a credential and harmonize these definitions across NIST standards.
- Define "identity," "digital identity," "digital identity data," and "identifier" and ensure these definitions are harmonized across all NIST documents and with international standards such as ISO/IEC 24760-3.
  - Currently VA uses the following definition for **Identity:** A set of attributes that uniquely describe a person within a given context. The set of physical and behavioral characteristics by which an individual is uniquely recognizable. SOURCE: VA Directive 0735
  - Need to differentiate between "identity" and "digital identity."
  - Define "context" as currently used in the definition for "identity/identifier."
- "Subject" is often used with the same definition as "subscriber", e.g. X.509 and related protocols.
  - Provide clear and harmonized definitions of "subject" and "subscriber."

Part 2: VA recommendations for NIST questions

NIST Question #4: What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

Recommendation: Include Privacy Enhancing Digital Identities

ISSUE: Existing government–centric privacy legislation and guidance are inadequate to protect individual privacy rights that are encapsulated in government and private sector systems, as witnessed by the EHR breaches and cybersecurity threats. Government-centric legislation includes Fair Information Practice Principles (FIPP) that have become "God and apple pie," not only for government agencies, but have been widely adopted by the U.S. Private sector. Moreover, existing privacy legislation such as the requirement that agencies perform a Privacy Impact Assessment (PIA) is government-focused and largely ineffective in preventing cybersecurity attacks. The existing legislation and solutions are not linked to security of personal identities.

Even in the healthcare industry, which has sector-specific privacy legislation (HIPAA Security and Privacy rule, Accountable Care Act and Population Health), digital identities are not sufficiently safeguarded. Breaches are commonplace, involving the compromise of millions of EHR records, including President Obama's, e.g., Anthem, and identity theft is rampant.

NIST ACTION: NIST needs to provide policy support for the new generation of privacy protections. There is no privacy policy guidance that attempts to safeguard one's digital identity. Government sponsored PIV, PIV-I, and PIV-Derived Credentials and their associated Levels of Assurance (LOA) are focused on verification and validation of the token, not on the digital identity of the individual.

Privacy here is defined as reasonable assurance of secure access to a person's Personally Identifiable Information (PII), the possession of a unique digital identity, and the relative sanctity of their Protected Health Information (PHI). An example of a definition of unique digital identity can be found in the draft language available from the NIST/IDESG Healthcare Working Group (HC WG).

The new generation of privacy protections includes frameworks and standards developed and piloted by Health Level 7, International, such as Data Segmentation for Privacy, Fast Healthcare Interoperability Resources (FHIR) - a draft standard for the exchange of resources which was recently piloted and demonstrated at the HIMSS15 and RSA meetings in April 2015 as "Privacy on FHIR."

Recommendation: Add a privacy component for each of the LOAs.

Make privacy considerations an integral part of each of the LOAs during the identity proofing process. This is especially important if there is any sharing of identity data between agencies.

Recommendation: Address privacy risks through user-centric risk assessment

As a consequence of being driven by a system-centric risk assessment, NIST 800-63-2 does not sufficiently address the privacy concerns of users. For the most part the document does not address core privacy principals identified by NSTIC (the TFPAP added some to the FICAM mix), but also fail to address privacy as it relates to selection of attributes to present to the world, e.g. a persona. For example, Steve operating as a private citizen (G2C) and accessing a government service has different privacy expectations than Steve, acting as an employee of a contracting company and accessing a government system as part of a job assignment. One size does not fit all. Definition of privacy

requirements and inclusion in certain profiles will enable identity services that meet a broader range of privacy needs.

Recommendation: Incorporate Privacy Terms

Suggest defining the following privacy terms in the updated model with standard definitions from international standards:

- **anonymity**
- **pseudonymity**
- **reversible pseudonymity**
- **unlinkability**

NIST Question #5: What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

Recommendations: Include the following:

- Derived credentials
  - Derived PIV-I?
- Biometrics
  - Biometrics should be a section in the document alongside Identity Proofing and Tokens. At high levels of identity assurance there is certainly a role for each of these different aspects of A&I. They answer the standard A&I questions (what you are, who you are, what you have, etc).
  - The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrollment and second or third factors on hard tokens. However, the trend in the industry is to unlock devices using biometrics with the task of binding the access request to a user to be performed by the verifier through the use of cumulative identity attributes that binds a device, location and behavior to an authorization request.
  - Add guidance on how biometrics can be used for each LOA.
- Additional devices that can be used as a token (i.e. mobile phone, smartcard chip on a credit card, FIDO compliant tokens)
- Add additional factors such as context factors and behavior factors (geo-location, IP address, MAC address, time of day, etc…)
  - We recommend extending the traditional three categories of authentication factors, currently: something you have, something you are, and something you know. NIST needs to enlarge the scope of authentication categories to include context and behavior to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a Key Chain.
- Vectors of Trust
  - The VOT at ietf.org list is for discussion of a common set of baseline "vectors of trust": common, orthogonal aspects of organization, technology and policy that help to determine the level of assurance that can be placed in a deployment of digital identity technology. Work will draw on deployment experience related to web

identity technology (eg. SAML, UMA, OAUTH and OpenID Connect) as well as experience with current state of the art in identity assurance. https://www.ietf.org/mail-archive/web/ietf-announce/current/msg13215.html

- FIDO standard
- Fair Information Practice Principles (FIPP)
  - Consent as part of authentication.
- Harmonize NIST SP 800-63 with work done in:
  - ITU-T X.1254,
  - ISO 29115,
  - ISO/IEC 24760-x,
  - HL7 Security WG,
  - OASIS TRUST Elevation,
  - OASIS Privacy Management Reference Model (PMRM),
  - OASIS Privacy by Design (PbD) WGs,
  - NISTIR 7817.
- Authentication in the cloud
- Guidance around security token services
  - Guidance is needed around the use of a Security Token Service. Such services can operate as a traditional Identity Verifier, but they can also act as a "translation intermediary" where someone shows up with one token type and leaves with another token type (for example). Include authentication-related guidance regarding, for example, what can and cannot be done during that "translation" to ensure the level of assurance remains the same (i.e., is not undermined/diminished).
- Identity as a service
  - To improve customer experience, enhance convenience, and increase the number of customers accessing VHA web sites, VHA is interested in mobile authentication, cloud-based proofing and authentication, and security token services. We suggest expanding 800-63 as necessary to provide guidance/insights in each of these specific areas.
- Non-person entity authentication
  - Currently, 800-63 focuses only on remote authentication of a human to a federal IT system. The VHA has significant need for authentication in various other contexts including non-person entity (e.g., device) authentication, system to system authentication in a service oriented architecture model, and data origin authentication. We suggest expanding the scope of 800-63 to provide guidance/insights on all logical access authentication contexts.
  - The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current trends. Given that mobile single sign technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign On support
- Anonymous/pseudonymous authentication

- In addition, VHA has significant need for authentication of anonymous or pseudonymous claimants. 800-63 does speak to those briefly, but we suggest adding any additional guidance/insights in those areas.

NIST Question #6: Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

Yes, VA feels that the representation of the confidence level in attributes should be standardized using a widely available format such as XML.

NIST Question #7: What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

Recommendation: Add Trust Elevation Techniques to 800-63 (next version)

It is recommended that Trust Elevation techniques should be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a CSP can authenticate a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user. The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per their own requirements and may be able to ask the CSP to do that on their behalf or combine the CSP tokens into application specific attributes, such as behavior, that they also can do on their own.

1. A standardized means of asking for higher assurance such as the ones being developed by OASI TRUST Elevation TC should be used.
2. An overlay/tailoring capability similar to SP 800-53 could also be used. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. In the overlays authentication strength can be computed using concepts form OASIS TRUST Elevation TC.

Social Security Administration

Below is a list of comments from SSA:

1. Remove the requirement to collect financial or utility account information at level of assurance 2 (LOA-2).

2. For the In-Person process, allow credential issuance at LOA-3 if the Government ID document confirms the address of record, but we cannot electronically verify the address.

3. Allow device recognition as a valid second factor, e.g., a cookie placed on the device.

4. Allow for a Look-up Secret Token confirmation on the device itself (e.g., Push notification).

5. Allow second-factors over the same primary e-authentication channel for LOA-2. For example, emailed second factor or OTP-generation algorithm running on the same device used for primary authentication.

6. Allow biometrics for specialized LOA-2 authentication scenarios, such as voice biometrics for authentication over telephonic channels, or fingerprint authentication for devices that support it.

7. Provide additional guidance and standardization for account management functions (e.g., helpdesk functions, password reset, etc.).

8. Standardize fraud detection controls and authentication error targets (e.g., maximum 'x' percent issuance False Positive rate at LOA-2).

9. Standardize the attribute assurances provided as part of the credential. This should also address confidence needed for attributes verified in the credential issuance process (e.g., what confidence do we need in the validity of a physical or electronic address to issue a credential at a given Level of Assurance to that address?).

10. Explicitly allow partial or zero-knowledge proofs in place of requiring users to enter sensitive information (e.g., allowing partial utility or financial account numbers in place of full account numbers).

11. Reduce the password entropy requirements (i.e., allow simpler passwords) when used as the knowledge-based authentication factor in a two-factor authentication scheme.

12. Update password entropy guidelines to reflect more recent industry standards and academic research (e.g., Weil, et al., Testing Metrics for Password Creation Policies). The complexity of our password requirements have long been a source of user complaints.

13. We suggest that in §§ 7.3.1.2 and 7.3.1.3, *Token and credential revocation and destruction*, that the requirement to "revoke or destroy" compromised credentials be changed to "revoke,

destroy, or disable". This change will allow temporary disablement of credentials that may be compromised. In these sections, we also suggest a recommendation to reduce the 72-hour revocation timeframe for compromised Level-2 credentials to not more 2 hours, and the 24-hour revocation timeframe for Level-3 credentials to not more than 30 minutes.

14. While we understand SP 800-63 is intended primarily as a technical guideline, we believe the inclusion of additional privacy considerations would strengthen the publication. For example, we suggest NIST mention the Fair Information Practice Principles (FIPPs) in the e-authentication guideline, perhaps in the Introduction, reminding readers to follow the FIPPs as they develop e-authentication solutions. We assume that any data protection guidelines are centered around the confidentiality, integrity, and availability information security principles.

15. It may also be beneficial to include, again in the Introduction, a brief discussion of the roles that various parts of an organization play in the development of e-authentication projects. For example, it is our understanding that most agencies do not include their privacy office in the risk assessment process; however, as an agency that does, we have found the practice to be extremely beneficial. In addition, proposed revisions to OMB's A-130 may increase the role of the Senior Agency Official for Privacy in some systems areas. Those and other changes to A-130, once published, should be reviewed as NIST considers revisions to 800-63. In addition, we note that additional guidance from OMB in support of the October 2014 Executive Order Improving the Security of Consumer Financial Transactions may impact 800-63. Finally, relevant guidance from NIST SP 800-53 Appendix J, Privacy Controls Catalog, should be considered when revising 800-63.

Jeremy Rowley

NIST 800-63 should be updated to permit the use of digital face-to-face schemes and make them the equivalent of in-person verification. Video conferencing software has advanced to the point where a face-to-face performed through skype, a google hangout, or similar process is of sufficient quality that a face-to-face performed electronically should be treated the same as an in-person face-to-face. Similar to a telephone verification, the session should be recorded and stored for the required period of time as evidence of the verification process.

Electrosoft Services, Inc.

Introduction to Electrosoft Comments

The comments and recommendations contained in this document represent those of the senior management and technical personnel of Electrosoft. Our team has interacted with 800-63 in a variety of different scenarios over the past several years. In our view it is vital NIST keep in mind the range of use cases 800-63 now supports when updating 800-63. Some direct use cases our team has leverage 800-63 include:

- Assisting federal agencies authoring internal policies
- Working with FICAM to understand the connect.gov requirements for Identity Providers, based on 800-63
- As a recommended best practice for commercial organizations
- As a recommended best practice for international governments and international companies. This was used as a means to standardize identity practices in use cases that involve users and organizations sharing information across multiple countries
- Assisting a new Trust Framework Provider (TFP) in authoring Operating Rules for their community and in applying as a TFP to the FICAM TFPAP process
- Auditing commercial identity providers against a security control document that is based on 800-63

Recommendations for Consideration in next 800-63 Iteration

1) **Recommendation**: Separate proofing and vetting LoA from technical security LoA aspects of the token

One of the fundamental recommended changes to 800-63 is a separation of identity proofing and vetting from the technical aspects of credential issuance and management. For example: in this model, a user could have a LOA 3 token with LOA 3 authentication protocol, along with a LOA 2 proofing and vetting. However, rather than marking the credential as LoA 2, it would be at the determination of the RP if the combination of factors is acceptable.

In our field experience with commercial deployments of credentials, this separation of credential strength and proofing and vetting is common. There are several real world use cases that necessitate this change:

- The FIDO Universal Authentication Framework (UAF) and Universal 2nd Factor (U2F) specifications should be reviewed to ensure they can be supported in SP 800-63 framework. This technology was not in existence when the last revision of 800-63 was released.
- There are government use cases which could necessitate this separation. Such an example would include a whistle blower scenario, where a trusted government office may want high assurance that they are getting information from the same token holder using a strong token, but the holder themselves remains anonymous.

- Strong tokens may be issued by an organization to their users, and then at a later date, the proofing and vetting associated with those credentials could be "stepped up" based on a subsequent process where the user demonstrates possession of the token. This provides the deploying organization greater flexibility in how to issue credentials to their users. It would also allow strong credentials that have already been issued to be "stepped up", thus extending their usability.

2) **Recommendation**: Update OMB 04-04 to support Recommendation #1: Separate proofing and vetting from technical security aspects of the token

OMB 04-04 will also require a revision to accommodate the idea that the token (strength, management, authentication, and assertions) are separate and distinct from the proofing and vetting of the user it was provided to, as the document is currently structured for a single assurance level.

3) **Recommendation**: Increased support for biometrics

In recent years, biometric technology has expanded as a means to authenticate users. This is particularly the case in the mobile world, where fingerprint readers as well as voice recognition capabilities have become standard features in many devices. It is clear these capabilities will be leveraged as authentication mechanisms within vendor products, and as such should be included in the SP 800-63 framework.

4) **Recommendation:** Harmonize Federal Bridge CP with 800-63 Requirements:

The delta between requirements at the same LoA in the FBCA CP and SP 800-63 results in conflicting guidance. This is particularly problematic in situations where existing PKI providers extend their services into non-PKI credentials, utilizing the same infrastructure and processes developed for PKI. In some cases (such as proofing and vetting policies) the conflicts results in a provider meeting all FPKI requirements, but not meeting 800-63 requirements. The position from providers is, if my process meets LoA 3 or 4 for FPKI, then it should be LoA 3 or 4 for 800-63 when issuing a non-PKI credential. From a provider's perspective, the government should have a single baseline set of requirements, resulting on them pushing back in their willingness to support 800-63 requirements that extend beyond FPKI requirements at the same level.

5) **Recommendation:** Enhanced Guidance for Privacy of Identity Transactions

Additional guidance on the privacy of user information should be addressed. In particular, there should be different requirements depending on the use case. If the user accessing the application is acting as an employee (G2G or B2G) they likely have different reasonable privacy expectations than if the same user is acting as a private citizen accessing an agency application (C2G). The nuances of how each of these scenarios impact what information is permitted in the transaction, and what can be logged and stored is not clearly identified.

800-63 related items that could use additional clarification

Addressing Permissible Use of Credentials and Identity Transaction Liability

One area of identity federation trailing the technical implementation is clear guidance on when a credential should be permitted for use. A PIV card may permit access to agency resources, and may even extend into accessing an external agency's resources. Can an agency allow the same credential to access a site promising discounts for government workers with a PIV card? What about access to a Federal Credit Union? What about using the PIV card to access a personal account? Without guidance on what is permissible use of PIV cards, onboarding federation partners becomes more difficult, as each use case that tries to extend the usage of PIV cards runs into the same permissible use debate.

In the PKI trust framework, there are "Limitations of Liability" in bridge CPs. CAs then agree to purchase insurance to meet the liability requirement as part of the cross certification prerequisites. As a result, both RPs and IdPs understand the financial risks involved in the transaction. In the non-PKI trust framework, this liability is largely left to bilateral contracts between IdPs and RPs. As agreement on the terms requires managerial and legal input, this process can be drawn out and stifle credential re-use. Just as there has been standardization of liability in the PKI space, the Federal agencies acting as a RP should have a similar framework for non-PKI credentials.

International Telecommunication Union (ITU) Study Group 17

This liaison statement represents a collaborative effort between the OASIS Trust Elevation TC and ITU-T Study Group 17, *Security*, in its Question 10/17, *Identity management architecture and mechanisms*, to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to its 9 April 2015 solicitation. (See http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html)

We also acknowledge and are grateful for the feedback and dialogue we enjoyed from participating experts of OASIS Trust Elevation TC, with whom we collaboratively developed this liaison statement, and who have been informed about this liaison statement.

I General comments

- As the solicitation notes, "NIST is considering a significant update to SP 800-63-2 in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication." Plainly that evolving threat landscape exists globally - with significant effects on the United States domestically. Thus, any update of this Special Publication should include extensive treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, NIST SP800-63-2 is completely devoid of anything other than U.S. domestic implementations, despite the agency's extensive international mandates in its Organic Act, the provision of international standards status to its publications, and the global nature of the authentication challenges being faced.[1]
- Levels of Assurance (LoA) today represents a range of trust depending on the order and the context of the evaluation of related assurance tokens. For example, if an authentication attempt comes from an unexpected location, a system may require the use of several sets of tokens even from the same LoA in order to ensure that the required assurance level is achieved. In many cases and in particular for knowledge based tokens. The attributes of these tokens losses value as a function of time. The advent of social media makes Knowledge Based Authentication (KBA) information public and water-down its effective use in the identification process
- Decouple Identity Binding
  - Permit identity proofing to occur after token issuance.
- Identity Register
  - Add to the model the concept of the Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that come with this role, including the protection of registration data for future dispute resolution balanced with user risk-mitigation goal of minimizing

[1] *See* National Institute of Standards and Technology Act, [available at http://www.nist.gov/director/ocla/upload/NIST-Organic-Act.pdf. *See also*, Organizations recognized according to Recommendations ITU-T A.4, A.5 and A.6, http://www.itu.int/en/ITU-T/extcoop/Pages/sdo.aspx.

instances of PII. The Identity Register may provide support for federated authentication and identification and credential reliability and recovery services.

- Risk Confidence Factors
  - Instead of grouping assurance profiles solely as 1,2,3,4 per OMB M-04-04 requirements, permit the expression of risk confidence score with multiple factors including identity proofing, token strength, multiple factors, biometric verification, etc.

II What requirements, processes, standards, or technologies are currently excluded from NIST 800-63-2 that should be considered for future inclusion?

- NIST should treat extensively used industry techniques such as the Extended Validation Certificates (EVcerts) pursuant to the CA/B Forum specification or the adaptation and extension found in ETSI TS 102 042 as means to combat threats to identity attributes and minimize man in the middle attacks.
- Rec. ITU-T X.1254 (ISO 29115) have done an extensive extension additions to the NIST 800-063 framework and need to be taken into consideration.

III Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

- OASIS Trust Elevation TC has developed three committee drafts that can be used for developing a consistent method for determining, evaluating and improving on LoA levels in a technology independent fashion. It is also developing metadata and protocol for expressing and exchanging needed trust elevation methods between a verifier and a client.
- Many systems are designed to support flexible authentication based on risk-based access. In many cases, these systems select many tokens from a given LoA to enhance the trust with the authentication step. NIST needs to be flexible and adapt the work from OASIS Trust Elevation TC in order to piggy-back on the use of common LoA metadata and trust elevation protocols that could work with IETF Oauth, OpenID Connect and OASIS SAML.
- At the point of transaction, the environment needs to be evaluated, not just the credential. NIST needs to start accommodating the latest trends in using a device as part of the authentication process. In this regard, the OASIS Identity-Based Attestation and Open Exchange Protocol Specification (IBOPS) models of enabling the user to authenticate to a device, and then an agent to attest to this fact, changes the dynamics of determining the LoA and the verifier (or CSP). Emphasis should be given to methods that lead to a hacker resistant authentication method where hacking the identity provider server will not result in massive security breaches. For example, in the OASIS Identity Based Attestation TC (IBOPS) models, the server holds a pointer to the client secrets and does not store any credentials locally. Client secrets are stored on the client device. This changes the attack vector of hackers whereby they will need to hack the server and the associated device to obtain a credential.
- Recommend harmonizing NIST SP 800-63 with work done in Rec. ITU-T X.1254, ISO 29115 and OASIS TRUST Elevation.

IV What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

- NIST SP 800-63 framework looks at the traditional three categories of authentication factors: something you have, something you are, and something you know. These categories are limiting because they assume strict and static authentication tokens with limited authentication capabilities. In many cases the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by an adaptive authentication engine. NIST needs to enlarge the scope of authentication categories to include context and behaviour to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a key chain. The trust level in the token can change based on the device health such as rooting or the use of anti-virus software. As such the achievable LoA from the device can vary with time and could be a function of software on the device and also a function of OS system integrity.
- The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrolment and second or third factors on hard tokens. However, the trend in the industry is to unlock devices using biometrics with the task of binding the access request to a user to be performed by the verifier through the use of cumulative identity attributes that binds a device, location and behaviour to an authorization request.
- The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current trends. Given that mobile single sign technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign On support.

V Threats to Authentication

- Increasing authentication assurance requires the combinations of authentication factors with no or minimal overlapping vulnerabilities can result in enhanced assurance. It is not the number of factors that matters but the reduction in threats that the combination of factors achieves. The way the combination occurs can either reduce or increase threats of context and related vulnerabilities. The OASIS Trust Elevation TC produced two committee drafts based on Recommendation ITU-T X.1254 (ISO 29115) that include a comprehensive list of authentication methods, and a way of computing the authentication strength based on vulnerabilities and their associated control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
- It is recommended that Trust Elevation techniques should be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a Credential Service Provider (CSP) can authenticate a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user. The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per their own requirements and may be able to ask the CSP to do it on their behalf or combine the CSP tokens into application specific attributes, such as behaviour, that they also can do on their own.

    - A standardized means of asking for higher assurance such as the ones being developed by OASIS Trust Elevation TC should be used.

- An overlay/tailoring capability similar to NIST SP 800-53 could also be used. Each NIST SP 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance to help each community of interest better meet its mission / business needs. In the overlays authentication strength can be computed using concepts form OASIS Trust Elevation TC.

VI Elevation of Biometric to a token

NIST does not recommend the use of biometrics as tokens. They are mainly used at enrolment. However, if the right privacy enhancing methods is used combined with appropriate trust elevation methods (like in OASIS IBOPS) biometric can be evolved to provide effective user authentication at least at LoA 2. So it is recommended that NIST investigate the use of biometric as a full token.

References: 4

1. OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC; https://www.oasis-open.org/apps/org/workgroup/trust-el/
2. OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC; https://www.oasis-open.org/apps/org/workgroup/ibops/
3. Recommendation ITU-T X.1254: Entity authentication assurance framework; http://www.itu.int/rec/T-REC-X.1254
4. Question 10/17 – Identity management architecture and mechanisms; http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q10.aspx

CDC

CDC has no comments to provide on the SP 800-63-2, *Electronic Authentication Guideline*.

Thank you for the opportunity to review and comment.

International Biometrics & Identification Association (IBIA)

The International Biometrics & Identification Association (IBIA) is pleased to provide comments on NIST Special Publication (SP) 800---63---2 *Electronic Authentication Guideline* in response to the NIST Call for Comments issued on April 9, 2015. IBIA is a non---profit trade association based in Washington, DC that promotes the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

Specifically, IBIA is providing comments in response to the following question raised by NIST in the Call for Comments: "What requirements, processes, standards, or technologies are currently excluded from 800---63---2 that should be considered for future inclusion?"

The current and prior versions of SP 800---63 define a very narrow role for biometrics in e---authentication. IBIA believes that a greater role for biometrics, as a legitimate authentication mechanism in e---authentication transactions, is now warranted in light of changes that have occurred since SP 800---63 was first published. The following rationale is provided for your review and consideration:

- This publication justifies the exclusion of biometrics as an authentication mechanism by stating that it is not "secret" and that the security of biometrics is "often weak or difficult to quantify". IBIA appreciates that biometric---based authentication systems used for e---authentication must be secure from attack. We believe that advances in biometric technology, such as anti---spoofing countermeasures, and other well--- understood security design approaches, such as server---based matching, digital signatures and encryption, make it possible to design effective systems that include biometrics as a recognized authentication token.

- We believe that biometrics should be designated as an authentication token for assurance levels 1 and 2. We believe that passwords and PINs are more likely to be compromised than biometrics. Obtaining a person's biometric template, even in clear text, is not the equivalent risk as obtaining someone's password or PIN since the impersonator is faced with the non---trivial task of inserting the binary biometric template data into the system as if it had been derived from a live image which was presented to a biometric sensor by the legitimate user. One can easily make the argument that biometrics are more secure than passwords or PINs and provide a significant convenience benefit to the user.
- There are a number of authentication architectures in which biometrics may be applied. These architectures should be investigated for suitability and included as appropriate, including server---based biometric verification. For example, NIST funded an NSTIC pilot that provided e---authentication based on specific mobile device possession (cryptographically verified) plus biometrics captured on a mobile device --- but matched within a server (i.e., at the verifier). The biometric data was cryptographically protected during transit and at rest, a comparative token risk assessment was performed, and the solution underwent security and privacy assessments as part of the pilot.
- Today, biometrics are being used in conjunction with mobile devices in multi---factor authentication implementations, not all of which strictly comply with the token definitions within SP800---63---2, but which demonstrate similar (if not better) risk profiles.

- The usability of biometrics has seen a huge improvement in the last decade, with commercial organizations beginning to adopt biometrics specifically for enhanced user experience (in addition to its security features). Having strong authentication that people can actually use is a significant advantage over many current technologies that are very difficult for people to use – in which case they don't. Server---based biometric matching has been used successfully as a second authentication factor in mobile banking and other financial services. Rather than adding "friction", as any strong authentication methods do, biometrics has been found to provide a very quick and easy user experience – even for the elderly. A recent article about the biometric e--- authentication implementation at the United Services Automobile Association (USAA) illustrates this point. See: http://www.americanbanker.com/news/bank---technology/biometrics---find---support---from---an---unlikely---demographic---seniors---1074341---1.html.
- Biometrics (the 3rd, 'what you are' factor) should be elevated to authentication token status. Where appropriate, suitable protection of the biometric data can be specified. If necessary, biometrics can be limited to use as a 2nd or 3rd factor only (rather than used alone as a single factor).

IBIA urges NIST to give serious consideration to defining an expanded role for biometrics in e---authentication applications – including server---based matching. If you have questions, please feel free to contact Tovah LaDier

Salesforce

Salesforce would like to thank NIST for the opportunity to comment on special publication 800-63. Before commenting directly, Salesforce would like to provide some context as to why we are commenting and why those comments are worth consideration. Salesforce serves over 150,000 customers globally. Salesforce manages over 1.5 billion successful authentications per month for over 100 million identities.

Salesforce takes a standards-based approach to identity. As a top tier SaaS application, we are part of over 10,000 SAML-based federated relationships. We are also using OpenID Connect, not only to facilitate social sign-on but also enterprise federation and service integration; we have also recently certified our OpenID Connect deployment against the OpenID Foundation conformance Configuration test profile. Salesforce has an OATH-based TOTP service as well. Salesforce also both client and server support for SCIM 1.1 Salesforce does more than just implenting the aforementioned standards; we take an active role in standards development. Salesforce is a co-author for multiple OAuth 2.0 profiles, major portions of OpenID Connect, and SCIM 1.1 and 2.0.

Salesforce serves US federal and state and local customers. Although Salesforce is not a FICAM-certified credential and token provider, we have an interest in growing our public sector market and view commenting on 800-63 as part of that effort.

Lastly, it is important to keep in mind that Salesforce is both a software-as-a-service (SaaS) and a platform-as-a-service (PaaS) vendor. As a platform provider, we make our identity services available to our customers and although aspects of 800-63 (and FICAM) are not directly relevant to our business, those same aspects may be relevant for our customers building on our platform.

What follows is Salesforce's response to the seven questions that NIST identified in its call for public comments.

1 - What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

This question is one of those areas where different mechanisms of establishing identity assurance are of different interest to Salesforce than to its customers. Salesforce approaches this perspective with the mindset that our customers establish assurance for their employees that are using our services. The methods by which that assurance is established is our customers' interest, not directly ours. The typical enforcement point for those requirements, especially regarding authentication, is at their corporate identity provider (IDP.) This response should be consistent with other platform providers' responses.

However, as a platform provider, we are asked by our customers to provide them ways to establish assurance for their customers. We observe our customers using fairly traditional means of establishing

assurance: identity proofing and authentication. The proofing techniques used are often dynamic knowledge-based authentication (KBA) based on services from the typical providers: LexisNexis, GB Group, etc. In some cases, customers are seeking proofing providers for specific professions ro constintuencies, notably doctors and other medical professionals. In terms of authentication, we see a combination of social sign-on (ostensibly based on username and password) and direct login to Salesforce again with username and password. Less common is the use of SMS to deliver one time passwords (OTP) as a second factor.

Important to note that risk doesn't directly factor into the deployment architectures when serving our customers. Customers want us, their platform provider, to be flexible in what we can deliver but rarely do they dictate specific stronger authentication requirements for their interactions with their customers and partners.

Lastly, Salesforce maintains a risk-based authentication engine which uses a combination of browser fingerprinting and IP range whitelists to establish risk. The risk calculation is a black-box to our customers and they can only influence the calculation by providing policies such as known-good IP ranges. However, this risk-engine is not employed when our customers' customers log into Platform delivered apps.

2 - Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

Such a separation already occurred. Identity assurance has already been split into proofing, credential issuance, and authentication. It is unclear the larger intent of this question in that regard. The weight that an organization gives to each component is their business.

One area that would be of service is to understand the of marginal utility of authenticators. The identity industry doesn't know how much stronger a credential is compared to another or combined with another. What is lacking is a language to describe a comparable metric. This lack of understanding has implications for level of assurance. For example, the industry doesn't know how different the level of identity assurance is for the use of username and password plus SMS-delivered OTP from a scenario in which the SMS-delivered OTP is replaced with an unphishable out-of-band challenge.

This lack of understanding presents two problems. First, as a platform provider, we can make educated guesses as to which authentication mechanisms we ought to offer and in which order should we ask for them. We'd like to think that our approaches are good ones, but because of the lack of comparability of authenticators, our approaches are still based only on our well-informed hunches and tests.

Second, our customers are left to fend for themselves in terms of selecting authenticators to help balance the identity assurance equation. They are also the front-line for authenticator usability. Our customers thus have to select authenticators that meet their risk requirements while delivering an acceptable user experience. Not having a model for authenticator comparison leaves them with simply comparing user experience. The majority of customers have neither the skills, budget, nor appetite to perform extensive usability analysis and testing, and this means they will often choose the authentication mechanism that is cheapest with their best guess regarding user experience. We, as an industry, ought to be able to better.

3 - What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

Salesforce does not have much direct experience in this domain. That being said, Salesforce does have at least one company offering remote proofing in our AppExchange. This company is using remote document capture as an ingredient to identity proofing.

4 - What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

The materials required to make a multi-channel contextually-informed authentication decision require participatory surveillance. Individuals must opt-in to sharing contextual information such as mobile device identity and location (both physical and geoIP). Novel signals for authentication include electronic signatures from a beating heart, icon location on a mobile device, and app-usage patterns. All of these "ingredients" for making authentication decisions come with their own privacy implications. In order for a person to be willing to submit to participatory surveillance, they must know what they get in return for their disclosures. Furthermore, they need assurances that the materials provided to help make authentication decisions are not retained.

When using mobile devices (as well as other connected devices surrounding the user) to gather contextual information, recognize that the device can attest to properties of the contextual information and allow the information itself to remain private, on the deivce. This is a pattern that 800-63 ought to endorse. Signals from mobile devices can and should be privacy-preserving (if not enhancing) but standardization of the pattern is required.

In regards to specific privacy-enhancing technologies, Salesforce believes that no specific technologies should appear in 800-63: Techniques, yes. Technologies, no. The risk of endorsing (even tacitly) a specific technology is that it freezes the market at a point in time until another revision to 800-63 occurs. Furthermore, if the technology endorsed (or even mentioned) is aspirational, notional, or simply a lab project, then agencies are left to implement something that might never be delivered. Case in point: zero-knowledge proofs.

Although ZKP hold much promise, there is little evidence that the vendors currently tinkering with it in the lab have the commitment from their management, product, and sales teams to make meaningful commercial efforts. Holding out hope against hope that a vendor will bring a ZKP system to market is an exercise in breath holding. That's not to say that the promise of ZKP isn't impressive, but waiting on it ignores incremental progress that can and must be made. From Salesforce's perspective working on privacy protections for risk-based authentication materials and participatory surveillance is time better spent.

Lastly, 800-63 should consider platform providers separately from individual deployments when exploring privacy requirements, technologies, and techniques. Privacy implications meant for an individual organization incorrectly applied to a platform provider limits both innovation as well as what

the platform provider's customers can do. As government moves towards shared-services within or without agencies, the privacy requirements on application platforms change. Said differently, the privacy requirements of an agency deploying a stack of technology is very different from an agency deploying a platform on which multiple agencies will run applications.

Using Salesforce as an example of this, we draw a very clear distinction between the services that we offer our customers and what they do with those services. For example, our platform can specify multiple scopes when interacting with social identity providers. There are legitimate reasons why our customers might specify broader scopes (and thus collect more information) than Salesforce provides as defaults. Not every customer has those requirements and it would be a poor choice for Salesforce, at the platform level, to restrict all of its customers. Applying more restrictive requirements at the platform level affects individual customers who have broader requirements and are free to act on those requirements.

5 - What requirements, processes, standards, or technologies are currently excluded from 800-63 that should be considered for future inclusion?

Salesforce has no comment on this question other than we believe that standards and techniques ought to be included and not specific technologies.

6 - Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

No. A representation of the confidence level in attributes should not be standardized because such a representation would lack the context of evaluation. What is a "stale" attribute to one party may be perfectly acceptable to another. Unless the complete context of evaluation could be represented, shared, and understood then representing the confidence level is not a useful exercise. Furthermore, few receivers of such information would have the maturity to do anything with the data and forcing them to do so would thwart adoption by adding complexity.

That being said, standardization of a schema for describing meta-attributes *might* be of use. A standardization of metadata regarding exchanged attributes could be of use. For example, if there was a standard schema to describe things such as "attribute last verified on" and "attribute verified by," then the receiving party could fold that metadata into its own evaluation processes. One approach would be to define a custom SCIM schema for this or an extension to the OpenID Connect User Info Endpoint. But again this might be useful to a small number of highly sophisticated receivers.

7 - What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

Methods need to be broken down into separate signaling and elevation techniques. Signaling techniques need to be finer-grain. In a TrustEl situation, bouncing the user all the way to their origination IDP to perform some form of stronger authentication is a terrible user experience and not particularly workable, especially in API-based and asynchronous interactions. Finding a way for an SP to signal and IDP to challenge the user without requiring a completely new session authentication would be better. This requires two signals: one from the SP to the IDP and one from the IDP to the individual. The SP-IDP interaction is likely more workable, especially as there is a cryptographic chain of trust between them. The IDP-User interaction is a bit trickier. A challenge request sent to the user without context looks suspiciously like a phishing attempt and this is especially true in API and asynchronous scenarios. If methods are to be created here, then user experience research is required if for no other reason then to prevent phishing-like and actual phishing behavior.

Regarding elevation techniques, one thing that is required is a sense for the marginal utility of authenticators. Having an SP ask an IDP (and thus potentially a user) for something stronger is fine so long as both agree to what stronger is and that stronger isn't going to annoy the user into abandoning the transaction or appear like a phishing attempt. It is possible that this requires a taxonomy of authenticator and authentication techniques. It would be good if an IDP can satisfy the TrustEl request through risk-based authentication without bothering the user, but if the SP doesn't understand the nature of the risk-based calculation then the IDP's interactions might not meet the SP's needs.

Salesforce again thanks NIST for the opportunity to comment on 800-63. If NIST has any questions or requires further clarification, please contact Ian Glazer

Pomcor

The following are seven comments by Pomcor on a possible revision of SP 800-63-2. They address three of the topics listed in the call for comments: privacy considerations (fourth topic in list), technologies to be considered for future inclusion (fifth topic), and trust elevation (last topic). Capitalized terms in the comments have the meanings assigned to them in SP 800-63-2.

*** COMMENT 1 ***

AUTHENTICATION WITH AN UNCERTIFIED KEY PAIR

A technique that may be considered for future inclusion is authentication with an "uncertified" key pair. In this technique, a computing device owned by a future Subscriber generates a random key pair to be used with only one Verifier and registers the public key with the Verifier. Later, the Subscriber demonstrates possession of the private key to authenticate as a repeat visitor, i.e. as the same party that registered the public key. If the key pair pertains to a digital signature cryptosystem such as DSA, ECDSA or RSA, possession of the private key can be demonstrated by signing a challenge derived from input from the Verifier.

(SP 800-63 defines a "Subscriber" as "A party who has received a credential or token from a Credential Service Provider (CSP)". The credential or token is verified by a "Verifier" for the benefit of a "Relying Party (RP)". When the credential is an uncertified key pair, the same party plays the role of CSP, Verifier and Relying Party.)

SP 800-63-2 considers the use of a key pair for authentication in Section 4.3, and a key pair is a component of a "Single-factor (SF) Cryptographic Device", a "Multi-factor (MF) Software Cryptographic Token", and a "Multi-factor (MF) Cryptographic Device" as defined in Section 6.1.2. But SP 800-63-2 only considers the use of a key pair when "A Verifier, knowing the Claimant[1]s public key through some credential (typically a public key certificate), can use an authentication protocol to verify the Claimant[1]s identity, by proving that the Claimant has possession and control of the associated private key token." (In SP 800-63-2 terminology, a "Claimant" is a party who claims to be a "Subscriber".) As we shall see below, the use of an uncertified key pair provides important privacy and security benefits that are not available when a key pair is part of a credential that asserts the Subscriber's identity and/or Subscriber attributes.

Authentication with an uncertified key pair is a versatile tool that can be used for many different purposes, including:

(a) Anonymous or pseudonymous authentication to a web site. The key pair is kept in the browser within HTML5 local storage controlled by JavaScript code downloaded from the site. In this usage, the uncertified key pair can be viewed as a drop-in replacement for a password, having the privacy benefits of a password without its security drawbacks.

(b) Anonymous or pseudonymous authentication of a native mobile application to its back-end. The key pair is kept in the native application's private storage or in key storage provided by the mobile operating system.

(c) Trust elevation with minimal disclosure. The Subscriber creates an anonymous account and uses an uncertified key pair for authentication. If and when trust is required, the Subscriber demonstrates possession of any required attributes (which may or may not uniquely identify the Subscriber) by means such as presenting one or more traditional cryptographic credentials or answering knowledge questions.

(d) Multi-stage identity proofing. An uncertified key pair can be used to establish continuity across multiple stages of an identity proofing process such as may be used for the issuance of a traditional cryptographic credential.

(e) Two or three-factor authentication. An uncertified key pair may be combined with a passcode and/or a biometric sample for two or three-factor authentication secure against physical capture of the Subscriber's device, as explained below in comments 2-4.

(f) Authentication to obtain an assertion. An uncertified key pair can be used for cryptographic authentication to a Verifier in order to obtain an assertion that can be presented to a Relying Party as discussed in Section 9 of SP 800-63-2.

(g) Protection of traditional credentials with virtual tamper resistance, as explained in comment 5.

*** COMMENT 2 ***

USING A PROTOCREDENTIAL AND A PIN FOR SECURE TWO-FACTOR AUTHENTICATION

A cryptographic credential can be used for two-factor authentication by requiring it to be activated by a passcode such as a PIN or a password, as discussed in Section 6.1.1 of SP 800-63-2. However, that requires protection of the cryptographic credential against an adversary who physically captures the Subscriber's device; otherwise the adversary can extract the credential from the device and use it without having to supply the passcode.

Two traditional techniques can be used for protection against physical
capture: tamper resistance, provided by a secure element within the Subscriber's device; or encryption under a key derived from the passcode, if the passcode is a high-entropy password rather than a short PIN.

A third technique becomes available if the cryptographic credential is an uncertified key pair. A "protocredential" can be stored in the Subscriber's device at registration time instead of the key pair; and the protocredential can be combined with the passcode to regenerate the key pair at authentication time. Thus the key pair is only present in the device when it is being used. In the case of a DSA key pair, for example, with the notations of the DSS, the protocredential may consist of the public paramenters p, q, and g, plus a secret salt.
At authentication time, the private parameter x is derived from the passcode and the salt using a key derivation function such as HKDF, and the public parameter y is computed as g^x mod p. If the key pair were certified, an adversary who captured the device and extracted the protocredential could mount an offline guessing attack against the passcode, testing guesses by deriving x, computing y, and checking if y is found in the certificate. If the key pair is uncertified and the public key is treated as a shared secret between the Subscriber and the Verifier, the adversary can only test guesses by attempting to authenticate online to the Verifier, who limits the number of attempts using a counter of consecutive

authentication failures. In the usual situation where the Verifier deals with multiple Subscribers, the counter to be used for each subscriber is identified by a key identifier that is part of the protocredential and is submitted by the Subscriber to the Verifier along with the proof of knowledge of the private key (and the public key, if the Verifier only retains a hash of the public key as registration time). The key identifier could be a record handle (such as a database primary key) that references a record in a database of Subscriber device records kept by the Verfier.

In this third technique, the protocredential can be stored without tamper resistance, and the passcode can be a short PIN, because it cannot be subjected to an offline guessing attack. The technique is therefore well suited for the case where the Subscriber's device is a small smart phone, which may not have tamper resistant storage easily available to applications, and where the size of the touch screen makes it impractical to type in a high-entropy password.

*** COMMENT 3 ***

JOINTLY HASHING A PUBLIC KEY AND A PIN FOR SECURE TWO-FACTOR AUTHENTICATION

In Section 6.1.3, SP 800-63-2 points out that multi-factor authentication can be achieved using multiple tokens, for example both a passcode and a cryptographic credential. When the cryptographic credential is an uncertified key pair, this multi-token technique can be greatly strengthened by letting the Verifier store a joint hash of the public key and the passcode, rather than a hash of the public key and a salted hash of the passcode. This prevents an adversary who breaches the security of the Verifier's database of Subscriber accounts from cracking a passcode with an offline guessing attack, assuming that the public key is treated as a shared secret between the Subscriber and the Verifier, as in the technique of Comment 2.
Passcodes are thus protected even if they are short PINs.

When the cryptographic credential is a certified key pair, joint hashing does not help, because the adversary can use the public key in the certificate to test guesses of the passcode.

The joint hashing multi-token technique has a security posture similar to that of the protocredential technique of Comment 2. With either
technique: (i) an adversary who captures the Subscriber's device and is able to extract sensitive data (the protocredential in one case, the key pair in the other) is not able to authenticate, assuming that the Verifier's database and the communication channel between the Subscriber and the Verifier are secure; and (ii) an adversary who breaches the security of the Verifier's database is not able to crack the passcode, assuming that the communication channel is secure.

*** COMMENT 4 ***

USING A BIOMETRIC KEY FOR BIOMETRIC PRIVACY PROTECTION

SP 800-63-2 allows the use of a biometric instead of, or in addition to, a passcode to activate a cryptographic credential and thus achieve multi-factor authentication. It also points out that a biometric is Personally Identifiable Information (PII), and that PII must be protected. But it does not discuss any methods for protecting a biometric used for multi-factor authentication.

A traditional method of using a biometric for activating a cryptographic credential stored in the Subscriber's device is to match a biometric sample obtained from the Subscriber against a biometric template stored in the device. This method is used, for example, for credential activation in a PIV card. But the biometric template is PII, and should therefore be stored in tamper resistant storage. This method is thus difficult to use in devices where tamper resistant storage may not be readily available to applications.

Several methods have been described in the academic literature that allow the use of a biometric for authentication while preserving biometric privacy without relying on physical tamper resistance. Some of those methods rely on a biometric key, which is consistently derived with moderatly high probability from varying but genuine biometric samples and non-PII auxiliary data. In one of those methods, used for example in the paper "Combining Cryptography with Biometrics Effectively" by F. Hao, R. Anderson and J. Daugman (IEEE Trans. Comput. vol. 55, no. 9, 2006, pages 1081--1088) the biometric key is generated at random at registration time and augmented with redundancy to create a codeword of an error correction system, which is x-ored with an enrollment iris code derived from an iris image obtained from the Subscriber to produce the auxiliary data. At authentication time the auxiliary data is x-ored with an authentication iris code derived from an iris image provided by the Claimant. The result of the two x-or operations is a bit vector that differs from the codeword at those bit positions where the enrollment iris code differs from the authentication iris code. Those bit differences are analogous to transmission errors over a noisy channel, which the error correction system is able to correct with moderately high probability if the iris image submitted by the Claimant is genuine, thus recovering the codeword. The original biometric key can then be recovered by removing the redundancy from the codeword.

A biometric key can be used instead of (or in addition to) a passcode to generate an uncertified key pair in the authentication method of Comment 2. The auxiliary data used to recover the biometric key at authentication time is then part of the protocredential. Since the auxiliary data is not PII, there is no need to store the protocredential in tamper resistant storage for biometric privacy protection.

A biometric key can also be used instead of (or in addition to) a passcode in the method of Comment 3 without requiring tamper resistant storage for biometric privacy protection.

*** COMMENT 5 ***

PROTECTING TRADITIONAL CREDENTIALS WITH VIRTUAL TAMPER RESISTANCE

The method of Comment 2 is a credential activation method that protects the credential against physical capture by not storing it in the Subscriber's device when it is not being used. At first glance, the method of Comment 3 does not look like a credential activation method, but is in fact functionally equivalent to the method of Comment 3.

The methods of Comments 2 and 3 can be used to protect an uncertified key pair against physical capture, but they cannot be used to protect a traditional authentication credential consisting of a certified key pair, i.e. a private key and its associated public key certificate, because they rely on depriving an adversary who captures the Subscriber's device of information that could be used to mount an offline attack against the passcode, and the adversary can find such information in the certificate. All the more, they cannot be used to protect certified credentials used for signing or decrypting email,

because both the certificates and the signed or encrypted email messages provide such information to the adversary.

However, traditional credentials used for authentication, email signing, or email decryption can be protected against physical capture by a method that we call "virtual tamper resistance". The method consists of encrypting the traditional credentials under a key-encryption key (KEK), entrusting the KEK to a cloud-based key storage service, and retrieving it from the KEK by authenticating to the storage service using the method of Comment 2 or Comment 3.

*** COMMENT 6 ***

USING A CONSENT MANAGER FOR PRIVACY PROTECTION IN ASSERTION-BASED AUTHENTICATION

In Section 9, SP 800-63-2 discusses authentication techniques where the Subscriber authenticates to a Verifier and obtains an assertion (in the Direct Model) or a reference to an assertion (in the Indirect Model), which the Subscriber uses to authenticate to a Relying Party (RP). These methods have a serious privacy drawback, in that the Verifier typically learns what RPs the Subscriber authenticates to, and the timing and details of each authentication to an RP.

SP 800-63-2 recognizes this drawback on page 96, where it says: "There are cases in which the RP should be anonymous to the Verifier for the purpose of privacy." Then it adds: 'The direct model is more suitable for the "anonymous RP" scenario since there is no requirement for the RP to authenticate to the Verifier as in the indirect model.'
However, in most if not all assertion-based authentication protocols the Verifier must redirect the Subscriber's browser to the RP in order to convey the assertion or assertion reference, and hence must learn at least the endpoint where the relying party receives the redirection. Furthermore, the Verifier should ask the Subscriber for consent to provide the information in the assertion to the RP, and in doing so should identify the RP to the Subscriber, which of course requires learning the identity of the RP.

This privacy drawback can be mitigated using existing technology by interposing a "Consent Manager" between the Verifier and the Relying Party. The RP redirects the Subscriber's browser to the Consent Manager with a request for one or more attributes. The Consent Manager identifies a party that can serve as both an authoritative CSP for the requested attributes and a Verifier. The Consent Manager asks the Subscriber for consent to request the attributes from the CSP/Verifier and redirects the browser to the CSP/Verifier, without revealing the identity of the RP. The CSP/Verifier authenticates the Subscriber and returns an assertion conveying the requested attributes to the Consent Manager. The Consent Manager asks the Subscriber for consent to provide the attributes to the RP, displaying the values of the attributes obtained from the CSP/Verifier, then redirects the browser to the RP passing the assertion. (One or both of the interactions between the Subscriber and the Consent Manager may be omitted for simplicity in some cases, according to policy and/or
configuration.)

It is essential for privacy that the Consent Manager be freely chosen by the Subscriber.

Use of a Consent Manager may be combined with other techniques in the above comments. For example, the Subscriber may first authenticate to the RP with an uncertified key pair, and the RP may later request attributes for trust elevation, as discussed in Comment 1. The Subscriber may authenticate

to the Consent Manager with an uncertified key pair, and to the Verifier with an uncertified key pair activated by a passcode and/or a biometric as described in Comment 2 and Comment 3.

*** COMMENT 7 ***

EFFECTIVE PROTECTION OF A LOW ENTROPY PASSWORD AGAINST ONLINE GUESSING ATTACKS

In Section 8.2.3, SP 800-63-2 describes throttling mechanisms for protection against online guessing attacks "when using a token that produces low entropy token Authenticators", such as when using a low entropy password (which is its own Authenticator). Table 6 requires a throttling mechanism to limit the number of failed online authentication attempts to 100 or fewer in any 30-day period.

But throttling mechamisms are vulnerable to a long term attack. If an attacker can make 100 guesses per month, he or she can make 1200 guesses in a year, and a fair number of low entropy passwords may not withstand 1200 guesses.

There is an alternative method of protecting a low entropy password against an online guessing attack that is much more effective, while also being less burdensome on the Subscriber.

The password is coupled with a username that is freely chosen by the Subscriber and can be changed at any time. (The Verifier uses internally a Subscriber number rather than the username as an immutable identifer.) The Verifier maintains a first counter of consecutive authentication failures that is reset when a correct password is entered, and a second counter of total failures that is only reset when the Subscriber changes his or her password.

The user is locked out when the first counter reaches a configured low limit, e.g. 5, and must use an out-of-band process to reset the password. If the limit is reached because of a denial-of-service attack, the user can change the username. (The Subscriber will initially choose an easy-to-guess username, but will choose a hard-to-guess one as an emergency when under attack, the change of username being accompanied by an investigation of the attack.)

An attacker may be able to time his or her online guesses to avoid ever reaching the limit before the Subscriber resets the first counter by entering the correct password. But the second counter is not reset by a correct password, and will eventually reach a configured threshold, e.g. 30. When the Subscriber logs in after the threshold has been reached, he or she is asked to change the password, and is not allowed to use the account for a purpose other than changing the password. The Subscriber may log out without changing the password, allowing the attacker to make more guesses, and may even log in and log out repeatedly. But when the second counter reaches a second threshold, e.g. 40, correct passwords entered by the Subscriber no longer reset the first counter. Thus there is a hard ceiling on the number of guesses that the attacker is able to make against a password before the password is changed (45 guesses if the first counter limit is 5 and the second threshold of the second counter is 40).

*** DISCLOSURE ***

Pomcor owns intellectual property related to the above comments.

Kaiser Permanente

Kaiser Permanente offers the following comments on the *NIST Electronic Authentication Guideline (800-63-2)* **("Guideline").**

The Kaiser Permanente Medical Care Program is the largest private integrated healthcare delivery system in the U.S., with over 10 million members in eight states and the District of Columbia.1 Kaiser Permanente is committed to providing high-quality, affordable health care services and improving the health of our members and the communities we serve.

We appreciate the opportunity to provide our feedback.

In general, we recommend a reorganization of the document into two main sections

1. A business-focused overview of levels of assurance (LOA) for registration/identity issuance and authentication, and guidance on LOAs appropriate to the types or risk levels of information being accessed, accompanied by a well-developed set of industry-specific, consumer-focused, end-to-end use cases for different industries, such as e-commerce, online banking, access to healthcare resources (patients and providers), and education. Use cases would address issues of identity proofing, ongoing authentication, and account recovery, and would include use cases which are mobile-centric. This would help enable development of comprehensive business architectures for identity access management systems which are domain-relevant.
2. A technical implementation guide which ties use cases to methods to allow for the development of identity access management systems which are standards-based and potentially interoperable, supporting the National Strategy for Trusted Identities in Cyberspace. The technical guide focuses on methods appropriate to the LOAs, as well as standards and best practices for implementing these methods.

1 Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., the nation's largest not-for-profit health plan, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 38 hospitals and over 600 other clinical facilities; and the Permanente Medical Groups, independent physician group practices that contract with Kaiser Foundation Health Plan to meet the health needs of Kaiser Permanente's members.

We also provide our perspective on a number of specific issues for consideration:

Give examples as to how LOA2 and LOA3 can be retained in account recovery workflows (e.g., describe how a LOA3 credential can be retained when someone needs to change, or has forgotten, a pin or password as one factor). Include specific guidance about account recovery methods for mobile-based services, and recommendations related to the caching of identity tokens on mobile devices.

Re-consider the role of dynamic Knowledge Based Authentication (KBA) in identity proofing for commercial identities. Could methods of KBA which increase guessing entropy (e.g., number of questions presented, domain of questions, permitted failures, information sources such as government/health/financial/private records, etc.) permit its use within an LOA3 schema for identity proofing? Note: within healthcare, the HIMSS Identity Task Force has made a recommendation mandating LOA3 for identity proofing for patient portal access which assumes dynamic KBA can be configured to provide LOA3-equivalent identity proofing.

Allow for more workflow flexibility for LOA2 and LOA3 identity proofing so goals can be achieved through equivalent paths. For example, when an Identity Provider has a pre-existing relationship with a customer, can there be flexibility in how an address of record is verified? Discuss in further depth how non-physical addresses, such as email and text messaging numbers, can be used for delivery of out-of-band codes—what alternate addresses are permissible and under what circumstances?

Consider expansion of the types of documents, including domain-specific documents, used as the basis of issuing identity credentials. For example, as an equivalent method, a health plan member wanting a patient portal account could electronically submit both address and health plan card information which is validated in real-time against a demographics database under control of the health plan without any obligation to submit Drivers License or other government-issued credential information.

What guidance can be given to adapting identity proofing and authentication schemas, by LOA, to the needs of people with motor and visual disabilities?

What is the role of adaptive authentication methods within the guidance? What methods of adaptive authentication would be permissible to confirm or elevate trust within an online session? Could aspects of adaptive authentication (e.g., confirmation of geo-location, confirmation of use of a “known” device) substitute for a traditional authentication factor in multi-factor authentication? Alternately, what guidance can be offered for in employing IP-based location restrictions as a filter prior to an authentication attempt?

Discuss when it is appropriate to use social media identity credentials for authentication to commercial services and when use is not advised. Provide guidance on “step-up” of identity proofing and authentication to allow use of social media identity credentials for commercial services.

Expand the concept of “equivalent means” (section 5.3.2) into more explicit statements about equivalency and the discretion Identity Providers can take in claiming equivalence to a given LOA. Expand the cited healthcare example to explicitly address a pathway whereby a health plan can serve as its own Credential Service Provider for purposes of e-prescribing of controlled substances.

John Hemphill

Request For Comments - NIST Electronic Authentication Update

I would like to add my comments to your request.

Now I'm a retired expat living in Ethiopia, but I still have an interest in this whole process of identity and trust and how it will play out in future cyberspace. My interest in this , is from that of a taxpayer concerned with finding common sense solutions to some huge problems and opportunities in fixing electronic authentication and the protection of privacy. The points I make are inter related. Some may not directly address the subject of electronic authentication.

I believe that a number of technologies should be working together. Consumers need to have the same access to strong credentials that the Federal government requires of it's employees, such as the PIV CAC cards. LOA 3 and 4 vehicles should be available to all for a fee, hopefully offset by some government subsidy and private monetization schemes, maybe to the 50$ level for an LOA 3 OTP PKI credential to maybe a 100$ for a biometric PKI LOA 4 credential. The credential should be like a license for conducting consequental business electronically. There should be a number of different public and private CPs to choose from, to avoid the paranoia surrounding a national identity system.

There should be a retail way to issue strong credentials for a fee or perhaps as a service from banks, Facebook, Verizon, US Post Office, State DMVs, etc. Make it cheap to obtain and mass promote the end of the username/password problem. NSTIC should be largely about making it easier to be obtain stronger credentiails for the public and proposing strong regulation to protect PII electronically or non-elecronicallu. Behind the scenes, drive the potential issuers of strong credentials to get busy, agree on the common rules and move together on forming the trust framework with appropriate trust marks (GTRI) to make it work. Maybe this is actually happening unknown to me. The banks, major communication carriers, etc. should be actively behind this in their own liability interests or the desire to be able to monetize the issuance and ongoing use of strong credentials. I know this will happen sooner or later. NSTIC should be there stirring the pot. Eventually, consumers will demand higher levels of identity as more of them get hacked. I am probably preaching to the choir, but there has to be a higher level of urgency attached to this, as the toll to the economy will only increase over time. With a baseline of higher level credentials available to the public, it will be far easier to implement more restrictive community of interest trust frameworks such as ones to cover organizations and people in the aerospace/defense industries. There is already some agreement on the acceptance of non federally issued credentials in the A/D world (Paul Grant - TSCP), probably

of benefit to the prime contractors like Lockheed.

Tie all the credential providers, IDPs, RPs, APs together in a trust framework that could be bridged to the Feds. As part of the trust framework, make membership dependent on trustmarks achieved that are NIST and community of interest standards. Find ways to quietly monitize the whole thing, so at least some of the costs are covered (ID Dataweb). I think generally that the Federal government has some greater interest in assuring the viability and security of the connected world, so there should be some cost sharing. I know this is a tall order but without a solid retail trust framework in place, we will still be stuck in the mud. Typically, the way I see it, consumers and RPs would have choices to make. If I'm a bank, say Wells Fargo. I say to my customers, in order to do online business with us, you will need to use LOA 3 mechanisms at a minimum. For high net worth customers, the bank may require a biometric LOA 4. Maybe as a customer of the bank, I desire to use LOA 4 to get in to my account even though I might only have 100$. Many different use cases depending on agreements made between consumers and RPs, depending on the perceived risks. Perhaps higher levels of assurance (LOA 5) could be invented to cover major transactions such as a home purchase where multiple parties are involved. Lots of interesting extensions could be imagined. I can see somewhere down the road where an education institution could be an AP, electronically attesting to the fact of whether a job applicant has a degree conferred by them. I am sure there are a large number of potential extensions of attribute provision electronically, once there is a mass availability of high levels of credentials.

To make a credential more attractive, it should be available as a derived credential on a person's mobile device. That's where a TPM capability would be helpful. I know the Feds are on the way to it, so why should the retail world be left out ?

Hardware roots of trust (TPM) should be widely available. People should be made aware of their existence and how to use them to obtain higher levels of security. Nothing in this area of authentication is 100 percent bullet proof, but obviously it should be significantly harder for a person's information to be discovered and exploited.

Something, I ran into with TSCP, was the work of ID Dataweb and their AXN and MAX ideas, where consumers could see actively who has been entrusted with their PII. That would be a big step forward as consumers have no idea of who knows what about them. As a side, I would include employers and others who routinely harvest PII, in this, with respect to what they need to know about someone dealing with them. Where I live and my SSN could and should be handled by parties who are properly trust marked. Most small organizations may not have an interest in obtaining those trust marks, so they should use services that are trusted to store PII. Maybe a new business opportunity ? The PII protection schemes should ideally be complete, so someone knows exactly who has what information about them. Obviously the IRS knows

more than you may like and there is no challenge to that, except for corrections. Maybe, I decide I am no more interested in using Facebook, so whatever I have shared with them should disappear. Lots of work needs to be done to assure the best PII handling. Legislation needs to be passed that defines PII, makes clear that it needs to be secured electronically and non electronically. Provide for tough incentives for organizations to fix their security holes, ie. big fines per consumer identity compromised. Without something tough, it's sloppy business as usual. Something more than a footnote in the corporate glossy for breaches.

Back to my original interest in the aerospace/defense world, I now see that paper distribution of policy restricted documents (ITAR/BIS) should he replaced by a system of view only display devices of various types. No way to download documents types for storage thus reducing the risk of exfiltration. Authorization to view, only with an LOA 4 credential accepted by the provider, ie. Lockheed, Army, Navy, Air Force, NATO, etc. Nothing stored on the sub contractor's system. Lessen the burden on the sub contractor for handling restricted materials. Viewing software and hardware is cheap. Save some trees in the process. All document access would be gated by active contracts or predetermined capabilities, per the Defense Contract Management Agency or authorized prime contractors. All contractors, governments and supply chain companies would be under the same trust framework, subject to appropriate auditable trust marks. Sounds tough, but anything less is a joke, in terms of protection for policy restricted materials.

TFS Program

TFS is seeing a need for componentization. Both commercial identity services and federal relying parties have expressed such interest to TFS. Ostensibly, componentization will give federal relying parties more flexibility in how they architect their solutions, especially in terms of what elements they outsource vs. what they perform in house. It will also allow federal relying parties to select best-of-breed identity services for each element of an overall solution or simply go with a single all-encompassing identity service. As a result of conversations with some TFS participants, we currently recognize the need for the following components:

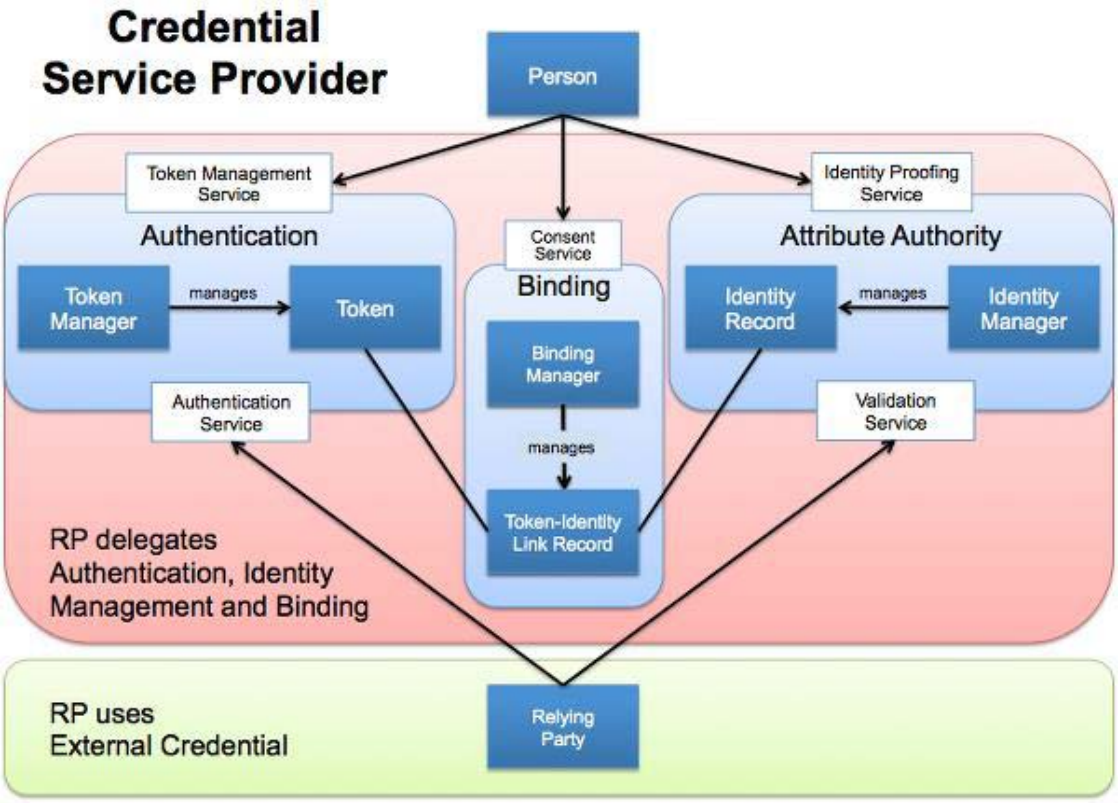
- **Token Manager (TM)**, which offers Token Management Services and Authentication Services
- **Identity Manager (IM)**, which offers Identity Proofing Services and Attribute Validation Services
- **Credential Service Provider (CSP)**, a full service that offers Token Management Services, Authentication Services, Identity Proofing Services, and Attribute Validation Services

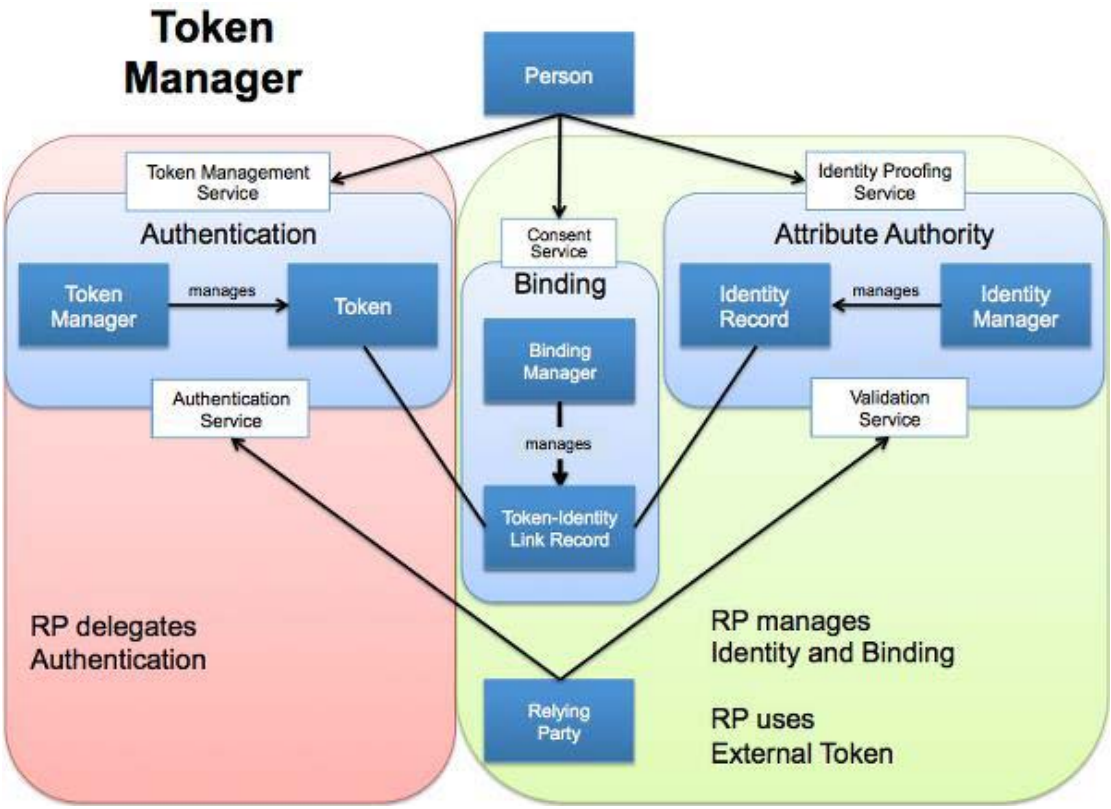
Of course, as lessons are learned over time, the list of components may need to change or existing components may need to be further broken apart.

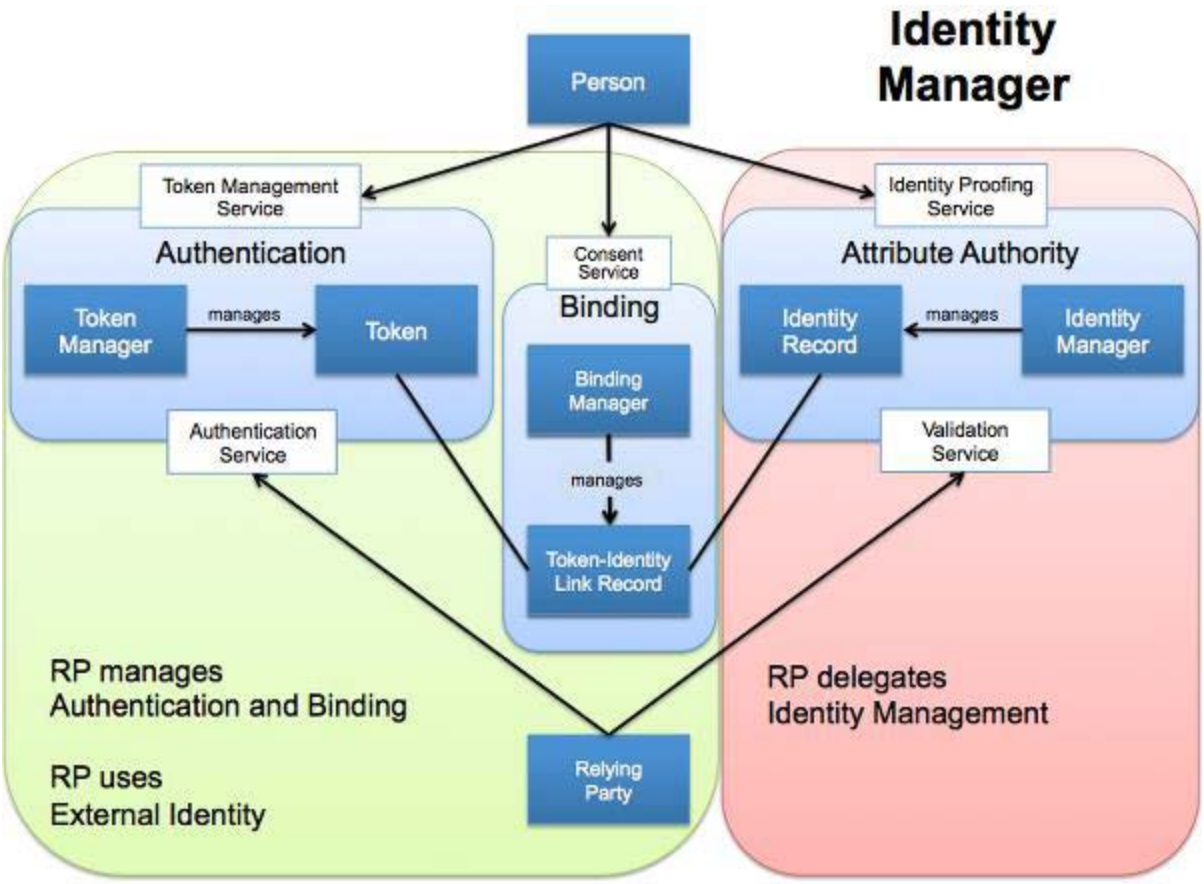
To support actual TM, IM, and CSP use within TFS, we are currently reworking the TFS document set, including the *Trust Framework Provider Adoption Process (TFPAP)* document that contains technical criteria based directly on NIST SP 800-63 requirements per LOA. Specifically, we are assigning the TFPAP technical criteria to applicable components.

Accordingly, TFS recommends enhancing NIST SP 800-63 to have each LOA[1]s complete set of requirements placed in tables that specify which components each requirement pertains to (something like a [3]meatball chart[2] with columns for the requirement and each of the components). We also recommend that NIST and TFS collaborate on a final assignment of requirements to components in order to harmonize the component approach and requirements assignment, and to optimize requirements specifically for TFS purposes. At that point, the TFS TFPAP may be changed to simply point to 800-63 rather than duplicate requirements.

Attached are the three TFS diagrams elaborate on the three components cited above.


Credential Service Provider
Person
Token Management Service
Identity Proofing Service
Authentication
Consent Service
Binding
Attribute Authority
Token Manager
manages
Token
Binding Manager
Identity Record
manages
Identity Manager
Authentication Service
Validation Service
manages
Token-Identity Link Record
RP delegates Authentication, Identity Management and Binding
RP uses External Credential
Relying Party


Token Manager
Person
Token Management Service
Identity Proofing Service
Authentication
Consent Service
Binding
Attribute Authority
Token Manager
manages
Token
Binding Manager
Identity Record
manages
Identity Manager
Authentication Service
Validation Service
manages
Token-Identity Link Record
RP delegates Authentication
RP manages Identity and Binding
RP uses External Token
Relying Party


Identity Manager
Person
Token Management Service
Identity Proofing Service
Authentication
Consent Service
Binding
Attribute Authority
Token Manager
manages
Token
Identity Record
manages
Identity Manager
Binding Manager
Authentication Service
Validation Service
manages
Token-Identity Link Record
RP manages Authentication and Binding
RP delegates Identity Management
RP uses External Identity
Relying Party

Internet Society

General remarks:

This section briefly summarises the key recommendations which arise from our responses to the NIST questions.

- NIST 800-63 is a US document – but it has a global, multi-jurisdictional impact, and that should be taken carefully into account in its revision. There is a strong requirement for trans-national interoperability, and this may require engagement in multiple stakeholder forums, both during and after the revision exercise.
- The Internet Society is an advocate for open, accountable standards development. We believe this is the appropriate way to develop and standardise widely-applicable frameworks for cross-border, interoperable services such as identity assurance.
- Large-scale, interoperable identity assurance frameworks must cater for the contractual and regulatory aspects of identity assurance as well as the technical aspects.
- The technical aspects should be underpinned by a clear framework for early and iterative interoperability and conformance testing.
- The assurance framework should embody privacy-enhancing principles such as (but not limited to):
    - Data minimisation
    - Selective attribute disclosure
    - User consent and control
    - User agency in a distributed environment

Context:

The Internet Society's role in Identity Assurance is as a convening body, a thought leader, and an enabler of technical standardisation (through its relationship with the Internet Engineering Task Force and its work with other standards bodies). We undertake technical work where we believe it will be most useful (for instance, in our support for the UnitedID[2] initiative, in Internet capacity-building, and in areas such as DNS and IPv6). The Internet Society also has a close association with the Kantara Initiative and that organisation's identity assurance work. One of our primary goals is to be a translator and a trusted advisor, between the technical and policy communities, giving a representative stakeholder view informed by our technical background.

However, the Internet Society is not, itself, responsible for operating an externalised identity assurance, IDP or authentication service on any significant scale. Accordingly, this response will be silent in those topic areas where the Internet Society has no direct, relevant deployment experience.

We welcome the opportunity to comment on the revision of NIST SP800-63. The original document had impact and application beyond its initially-intended scope, and we expect the revised version will do the

2 http://unitedid.org/about/challenge/

same. Accordingly, we hope that this revision will be seen as part of an iterative cycle. Just as the existing framework set out by OMB 04-04 and NIST SP800-63 has, over time, revealed shortcomings, so we expect that the current cycle will result in a framework which will need revision in the future, as technology and practice continue to evolve.

Topics:

NIST#1:

What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

ISOC#1:

- What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction?

An instructive example of service/transaction-related risk management can be found in the Scandinavian Bank-ID system. It is instructive because it was the first authentication scheme to rely on identity assurance processes in one sector (banking) in support of authentication in another (public sector service delivery). Experience has shown us that identity assurance schemas are more likely to be successful if they can be used to assess different identity infrastructures in multiple sectors (conversely, an identity assurance schema that can only be applied to a single sectoral infrastructure is of limited use).

Our subsequent comments on NIST#1 apply to identity assurance schemas in general, rather than to Bank-ID in particular.

As a general observation on security, privacy and usability: the NIST schema based on the four levels of assurance (and its UK counterpart) has been effective in providing at least a basic, consistent and quantifiable framework for matching security, privacy and trust to a manageable set of risk levels. The New Zealand government’s approach, of assigning a “score” to various forms of identity assurance evidence (the so-called “breeder documents”), and accumulating evidence until it reaches one of a defined set of threshold values, adds granularity and flexibility to the basic 4-LOA model.

- How do they differentiate trust based on risk?

When public key infrastructures were first attempting large-scale deployment, a significant difficulty was the question of how to apportion liability in case something went wrong. Certificate authorities were seen as the root of trust, but they rejected the assertion that they could legitimately be held liable for transactions subsequently executed using the keys/certificates they issued. The business model could not evolve successfully until a distinction was drawn between two principal forms of liability:

Liability arising from the operation of a certificate authority (secure storage of the CA's private keys; generation and use of strong keys; integrity of the certificate generation process);

Liability arising from the subsequent use of keys/certificates in support of transactions.

It is a good principle for an identity assurance framework to be capable of transposing this approach into the authentication context. The identity issuers/proofers in the scheme accept a certain level of liability relating to initial identity proofing processes, and for the integrity of the credentials issued as a result. However, a well-designed scheme will be able to separate this from liability arising out of subsequent use of the credentials – for instance, for the use of bank-issued credentials in a public sector service delivery context.

- How is interoperability of divergent identity solutions facilitated?

The phrase “identity solutions” is vague in this context. However, assuming a broad definition (identity assurance technology and practice), interoperability is best facilitated through the following measures:

- A clear focus, from the outset, on the contractual and regulatory aspects of interoperability, in addition to any technical interoperability measures. This has been a characteristic of large-scale technical interoperability initiatives over the past 20 years - such as the Secure Electronic Transaction (SET) consortium, the Identrus initiative and the Liberty Alliance. All of these devoted significant time and effort to addressing the contractual and regulatory foundations of interoperability, in addition to that devoted to the technical aspects.

- The ability to take a global, multi-jurisdictional perspective. The Internet transcends national borders, and at both regional and national levels there is a clear requirement for cross-border interoperability in identity assurance approaches and mechanisms. This is best achieved through early and regular engagement with the appropriate stakeholders, and may require engagement in more than one forum (for instance, the IDESG, the IETF, the OECD and the IGF could all be expected to have relevant views on interoperability, but different contextual perspectives).

- An open, accountable approach to standards definition. The Internet Society's role as the hosting organisation of the IETF is clear; in our view, it represents a model for the open development of globally-applicable open standards. In areas such as government identity

assurance there are bound to be country-specific aspects (US PIV credentials being an example), but experience suggests that it is wisest to situate these in a meta-model which, in principle, can bridge the gaps between different country-specific schemes. As evidenced by its support for the OpenStand[3] initiative, the Internet Society endorses a clear set of five principles for the development of standards.

- The ability to conduct practical interoperability tests, particularly between different technical implementations of defined standards and processes. Again, experience through initiatives such as the Identrus consortium and the Liberty Alliance indicates the importance of removing as many barriers as possible to the early and iterative testing of different vendors' products against each other and the defined standards.

NIST#2:
Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

ISOC#2:

Identity assurance processes and identity assurance technologies should be separated into two discrete, but related disciplines (a principle already adopted by OMB 04-04 and NIST SP800-63).

Processes and technology could then be analysed following a time-line approach which reflect the "chain of trust" inherent in any credential or attribute assurance program.

As a non-exhaustive example, the time-line should account for at least the following stages:

- Registration, Verification and Enrolment (RVE) – sometimes also called "identity proofing"
- Credential production and issuing
- Authentication and authorisation processes
- Credential lifecycle management (production and issuing; validation; amendment; replacement; revocation; destruction).

This would allow the construction of a comprehensive model, at each step of which the impact of different levels of assurance could be gauged.

NIST#3:

[3] Open-stand.org: https://open-stand.org/about-us/principles/

What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

ISOC#3:

We believe that a fundamental principle, here, should influence NIST's approach to identity assurance in general.

Current approaches to identity assurance (particularly in the government sector) adopt an essentially retrospective approach. "Identity" (or, more accurately "a credential"), is something conferred on an individual by a trust authority through what Kim Cameron has referred to as a "trusted ceremony". The acceptance of subsequent assertions of identity hinges on that initial trustworthy step, and the integrity of the subsequent steps (see the credential lifecycle listed above, under ISOC#2).

However, the Internet gives rise to a quite different, parallel model of identity. Internet-based service providers may well "identify" a given user through longitudinal linking of many attributes, whether or not the sources of those attributes are particularly trusted. This is a less linear and less retrospective model, in which the roots of trust are more distributed and more varied. The trust and assurance frameworks that evolve from current practice will be deficient if they do not take account of this new model.

The Internet Society has helped to initiate, through the IETF, a discussion group working on the various elements (technical and otherwise) that underpin online trust. We would welcome the participation of other stakeholders in this exercise, which has been labelled "Vectors of Trust"[4]

NIST#4:

What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

ISOC#4:

First, the previous comment (ISOC#3) implies the greater role played by general attribute data (as opposed to pure identity attributes) in contributing to the "identifiable digital footprint" of any given individual.

---

[4] https://www.ietf.org/mailman/listinfo/vot

One privacy-enhancing principle that should be built into the identity assurance architecture, therefore, is the ability to support selective release of trustworthy attribute-level assertions. Again, referring to the previous comment (ISOC#3), current identity assurance systems have evolved on the basis that they must cater for a specific set of distinguishing attributes (typically: first name; last name; date of birth; place of birth; gender). Identity assurance consists of validating these attributes and encapsulating them in the form of credentials.

Selective attribute release depends on the ability to capture and then assert individual attributes, whether or not they uniquely identity the data subject. Privacy requirements are not met if, in order to satisfy a single-attribute release, or to release just the attributes required to inform a particular access decision, the data subject has to disclose a fuller set of attributes to the relying party. Examples of this abound, but generally speaking a user often only needs to release attributes relating to role or affiliation in order to gain access to a resource.

Second, the Internet is increasingly characterised by loose-coupling of online services. A major source of so-called “disruptive” innovation is the increasing ease with which existing value chains can be shortened or bypassed. For example, social networking credentials might be used to access a VOIP service.

The ability to construct loosely-coupled services, in turn, opens up the potential for intermediary actors (of all kinds) to create a niche in the value chain. This is relevant to the assurance/privacy topic because we can expect individuals' attributes, increasingly, to be in the hands of intermediary actors and/or devices. If those intermediary functions form part of a clear trust framework, the resulting architecture will be usable in trustworthy ways. If they do not, the resulting architecture will fail to server the privacy interests of the data subject.

The identity assurance framework should therefore consider how attribute data can be managed in trustworthy ways, when it is in the hands of neither the data subject, nor the originating actor, but a third party intermediary. The framework should also consider how a relying party can cater for attributes, and attribute sources, of different levels of trustworthiness.

Third, the intermediary-based architecture described above can be expected to span geographic boundaries (it already does). Again, the identity assurance framework should consider the trust implications of this, not least from the standpoint of the data subject.

Several of these issues have already arisen, historically, in slightly different forms, because of cross-border data transfers and cloud service provision.

Arguably, current regulatory models (such as, but not restricted to EU-US Safe Harbour) have failed to provide an adequate framework, since they allow the transfer of data from stricter regimes to more permissive ones where it may be used in ways that would not be permissible in the originating regime[5]. Where identity assurance architectures are built across the same national and/or contractual boundaries, such failures will have a greater impact.

NIST#5:

What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

ISOC#5:

We have two principal comments in response to this question. The first is an observation about trust elevation versus its corollary. The second reflects other stakeholders' view that the current 4-LOA model was a worthy start, but has proved insufficiently granular in practice.

First, we note that the current framework does consider the implications of trust elevation. A typical use-case is that a user starts by browsing for information anonymously, but then reaches the point where she wishes to transact – at which point the trust level is elevated by requiring the user to authenticate. Another common use-case is that a user authenticates at a low LoA (typically username/password) which is sufficient for certain actions, but then wishes to perform a higher risk transaction – at which point the trust level is elevated by mechanisms such as Knowledge Based Authentication (KBA) and/or additional authentication factor(s).

The user experience is a factor, here. If a user can be misled into believing that she is in a trustworthy context when she is not, she may be fooled into entering authentication credentials, or exposing a userID/password, or disclosing inappropriate personal data, when she should not do so. Good design

---

[5] Feb. 2015: German data protection commissioners to take action against Safe Harbor - https://www.techdirt.com/articles/20150205/10022729919/german-data-protection-commissioners-take-action-against-eu-data-transfers-to-us-under-safe-harbor-program.shtml

May 2015: Belgian privacy commission threatens Facebook with legal action over tracking - http://www.theguardian.com/technology/2015/may/15/facebook-must-stop-tracking-users-non-users-legal-action

practice will avoid putting users in this position (though good practice in this area is not always adopted, as any successful phishing attack demonstrates).

However, much less attention has been paid to the "trust degradation" user experience. That is, the user experience appropriate to cases where a user *has been* transacting in a trustworthy context, and then reverts to a lower level of trust. At this point, it is key that the user should understand the downwards shift in trust. Otherwise, thinking that she is still in a high-trust context, she may be fooled into making an inappropriate disclosure. Unfortunately, this design principle is often either not recognised or is sacrificed in the name of "seamlessness", in an attempt to make the UX as consistent as possible when transitioning between trust levels. Good practice in this area could be improved and propagated.

Second, as other stakeholders have pointed out, the current 4-layer model has proved not to align with actual deployment practices, and to be too inflexible to accommodate "LOA 1.5, LOA 2.5" and so on. However, as these requirements are dealt with in more detail in the responses from deploying organisations, we will not revisit them here.

NIST#6:

Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

ISOC#6:

We believe that assurance considerations are a logical consequence of the developments described in ISOC#3 and ISOC#4 above. An identity assurance framework which *cannot* accommodate attribute-level assurance parameters will be deficient. Note that this is not to say every user of the framework is thereby obliged to make use of this function.

We are aware that there is a contrary view, that the concept of attribute-level assurance is nonsensical from the outset. According to this view, attributes are trustworthy because they come from a trustworthy source, and their trustworthiness is the trustworthiness of the source, not the attribute itself. We believe the modern Internet already gives rise to use-cases which demonstrate that this model falls short.

Example:

> Roger runs an app which, as long as he is online, instantly updates his location using the network data available to the device. The app relies on device functionality, and the device, in turn, relies on the network infrastructure. Neither the app nor the device have any reason to regard their data sources as inherently untrustworthy.

However, when Roger goes offline, the device loses its ability to update location. It can still pass a location attribute to the app, but the device "knows" that the less fresh that data is, the greater the risk that it is untrustworthy. As far as the app is concerned, the device is still a perfectly trustworthy *source* of data, but the attribute it passes becomes more unreliable over time.

If the architecture supported it, the device *could* pass a trustworthiness qualifier along with the attribute. If the architecture has not been designed with this possibility in mind, the function is harder and more expensive to retrofit.

There are many other possible applications of this principle (for instance, in gauging the trustworthiness of a key/certificate since it was last refreshed).

As to the format of such attribute assurance data, a sound principle is that it should be technology-neutral as far as possible, and standardised through an open process. However, work in the W3C suggests that there may be alternatives to an LOA-based model for assurance of assertions. One proposal is to state the provenance of a given assertion, e.g. by tagging the attribute, so the relying party can decide whether or not (and to what degree) to trust the source of the assertion. The integrity of the provenance field could be cryptographically protected by digital signing. [6] In the identity management field, this approach is implemented in the form of metadata exchanges between federated identity providers – it is possible that similar lessons could be learned from provenance ontologies used in other fields.

NIST#7:

What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

ISOC#7:

ISOC does not have performance data applicable to this topic.

However, we believe that the principles outlined in previous comments (specifically, ISOC#3 and ISOC#4 on the emerging models of loosely-coupled, and attribute-based identification, and ISOC#6 on attribute assurance) are relevant to the question of how to increase assurance levels within a transaction.

6 For example, this possible solution was raised in the W3C Provenance Working Group Connection Task Force Informal Report at http://www.w3.org/2011/prov/wiki/Connection_Task_Force_Informal_Report

OASIS Trust Elevation & ITU-T SG 17

This work represents a collaborative effort between the OASIS Trust Elevation TC and ITU-T SG 17 Identity Management Question (Q10/17) to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to its 9 April 2015 solicitation. (See http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html)

I. General Comments

- As the solicitation notes, "NIST is considering a significant update to SP 800-63-2 in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication." Plainly that evolving threat landscape exists globally - with significant effects on the United States domestically; thus, any update of this Special Publication should include extensive treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, SP800-63-2 is completely devoid of anything other than U.S. domestic implementations, despite the agency's extensive international mandates in its Organic Act, the provision of international standards status to its publications, and the global nature of the authentication challenges being faced.[7]
- Levels of Assurance (LoAs) today represents a range of trust depending on the order and the context of the evaluation of related assurance tokens. For example, if an authentication attempt comes from an unexpected location, a system may require the use of several sets of tokens even from the same LoA in order to ensure that the required assurance level is achieved. OASIS Trust elevation TC has taken a close look on how to enhance trust for these uses cases and we do recommend that NIST try to harmonize with the work.
- SP800-63-2 is significantly directed at U.S. Federal Systems under activities shared with the Department of Homeland Security (DHS). DHS recently transferred several key platform specifications for cyber threat intelligence sharing to a new OASIS Technical Committee for Cyber Threat Intelligence (CTI). OASIS TC Trust-el intends to collaborate closely with CTI on implementations to reduce electronic authentication threats. NIST's evolution of SP800-63-2 would likely benefit significantly from DHS incorporating these CTI platforms into future versions of the specification
- Identity Register
    - Add to the model the concept of the Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that come with this role, including the protection of registration data for future dispute resolution balanced with the user risk-mitigation goal of minimizing instances of PII. The Identity Register may provide support for federated authentication and identification and credential reliability and recovery services.

---

[7] *See* National Institute of Standards and Technology Act, [available at http://www.nist.gov/director/ocla/upload/NIST-Organic-Act.pdf. *See also*, Organizations recognized according to Recommendations ITU-T A.4, A.5 and A.6, http://www.itu.int/en/ITU-T/extcoop/Pages/sdo.aspx.

- We recommend that NIST consider the identity and access management architecture to be addressed at a much higher level of abstraction and to separate identity management from access management.

II. What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

- NIST should implemt extensively used industry techniques such as the Extended Validation Certificates (EVcerts) pursuant to the CA/B Forum specification or the adaptation and the additional token extension found in ETSI TS 102 042 pursuant to European Union policies as means to combat threats to identity attributes and minize man in the middle attacks. The Forum's recent inclusion of extensive government entity trust certification provisions in the specification, facilitates the use of EVcerts for a broad array of new government services
- NIST has done a great job in harmonizing its work with other stanadrds and in this siprit we do recommend continued harmonizations with ITU-T X.1254 (also ISO 29115) work that has done extensive extensions to the 800-63 framework . In particular, the ITU-T X.1254 (also ISO 29115) work relating to non-human entities .

III. Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

- OASIS Trust Elevation TC has developed three committee draftes that can be used for developing a consistant method for determining, evaluationg and improving on LoA levels in a technology independdent fashion. It is also developing metadata and protocol for expressing and exchanging needed trust elevation methods between a verifier and a client.
- Many systems are designed to support flexible authentication based on risk-based access. In many cases, these systems select many tokens from a given LoA to enhance the trust within the authentication step. NIST needs to be more flexible and adapt the work from OASIS Trust Elevation TC in order to piggy-back on the use of common LoA metadata and trust elevation protocols that could work with Oauth, OpenID Connect and SAML.
- At the point of transaction, the environment needs to be evaluated, not just the credential. The threat environment affects the trustworthiness of the transmitted credential.
- NIST needs to start accommodating the latest trends in using a mobile device as part of the authentication process.
    - As an example, the OASIS Identity-Based Attestation and Open Exchange Protocol Specification (IBOPS) models of enabling the user to authenticate to a device, and then an agent to attest to this fact, changes the dynamics of determining the LoA and the verifier (or CSP).
- Consideration should be given to hacker resistant authentication methods, e.g., where hacking the identity provider server will not result in massive security breaches.
    - For example, in IBOPS, the server holds a pointer to the client secrets and does not store any credentials locally; client secrets are stored on the clinet device which changes the attack vector whereby hackers will need to hack the server and the associated device to obtain a credential.

IV. What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

- NIST SP 800-63 framework looks at the traditional three categories of authentication factors: something you have, something you are, and something you know. These categories are limiting because they assume strict and static authentication tokens with limited authentication capabilities. In many cases the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by an adaptive authentication engine. NIST should enlarge the scope of authentication categories to include context and behavior to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a Key Chain. The trust level in the token can change based on the device status/health such as rooting or the use of anti-virus software. As such, the achievable LoA from the device can vary with time and could be a function of software on the device and also a function of OS system integrity.
- The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrollment and second or third factors on hard tokens. However, the trend in the industry is to use biometrics more broadly. For example, biometrics can bind the access request to a user as part of a larger process performed by the verifier through the use of cumulative identity attributes that binds a device, location and behavior to an authorization request.
- The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current environments. Given that mobile single sign-on technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign-On support.

V. Threats to Authentication

3. Increasing authentication assurance requires the combination of authentication factors with no (or minimal) overlapping vulnerabilities to enhance assurance. It is not the number of factors that matters, but the reduction in threats that the combination of factors achieves. The way the combination occurs can either reduce or increase threats of context and related vulnerabilities. The OASIS Trust Elevation TC produced two committee drafts based on ITU-T X.1254 (ISO 29115) that include a comprehensive list of authentication methods and a way of computing the authentication strength based on vulnerabilities and their associated mitigation/control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
4. It is recommended that Trust Elevation techniques be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a Credential Service Provider (CSP) authenticates a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user. The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per

their own requirements and may be able to ask the CSP to do it on their behalf or combine the CSP tokens into application specific attributes, such as behavior, that they also can do on their own.

a. A standardized means of requesting a higher assurance level, such as the ones being developed by the OASIS Trust Elevation TC, should be used.
b. An overlay/tailoring capability similar to SP 800-53 could also be used. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance, to help each community of interest better meet its mission / business needs. In the overlays, authentication strength can be computed using concepts form OASIS Trust Elevation TC.

VI. Elevation of Biometric to a token

NIST does not recognize the use of Biometrics as authentication tokens. They are mainly used at enrollment. However, if the right privacy enhancing methods are used, combined with appropriate trust elevation methods (e.g., as in OASIS IBOPS), biometrics can be evolved to provide effective user authentication at least at LoA 2. It is therefore recommended that NIST investigate the use of biometric as a full token.

References

1. OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC; https://www.oasis-open.org/apps/org/workgroup/trust-el/
2. OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC; https://www.oasis-open.org/apps/org/workgroup/ibops/
3. X.1254 : Entity authentication assurance framework; http://www.itu.int/rec/T-REC-X.1254/en
4. Question 10/17 – Identity management architecture and mechanisms; http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q10.aspx

SAFE-BioPharma Association

I. Unstructured Comments

A. NIST must recognize that SP 800-63 is more than a US government only document. It is also mandatory for private sector entities that must do business with the government and thereby spreads into the B2B space seamlessly as a de facto standard for determining the trustworthiness of online assertions of identity. Therefore, NIST has an obligation to make sure that any changes to this document do not disrupt existing business processes without sufficient collaborative input, justification and lead time.

B. In overall concept, SP 800-63 was designed to provide guidance to Agencies for implementing risk mitigation strategies based upon the OMB M-04-04 four level model for determining risk. The mitigations were structured to align exactly with the risk model. In the subsequent 11 years, however, other, more precise models have emerged for determining risk and risk mitigation and other factors have been identified in addition to the classic 3FA. NIST publications in the interim have gone some way toward addressing this situation, primarily in the SP 800-53 series of controls related to identity and access management, however, SP 800-63 continues to address only the OMB risk model. As a first step, in order to continue its extremely valuable function of identifying mitigation strategies for authentication risks, NIST should incorporate appropriate SP 800-53-4 controls into the next round of SP 800-63 revisions and should include current thinking about risk, risk vectors and risk mitigation strategies. Generalizing token requirements from X.509 (without abandoning it!) is also a priority.

C. NIST should continue its process of aligning with EU and ISO policies and standards to the extent possible in international collaboration.

D. There is nothing intrinsically wrong with a 4 LOA model, despite opinions to the contrary. The EU has recently adopted a 3 LOA model (where NIST LOA-1 is implicit as below the eIDAS “Low”), and many US allies among others have adopted it successfully. Therefore, in fact, abandoning this model is unlikely to result in any realistic improvement to the overall trust models in production. Expanding analysis of what constitutes comparability with each LOA from the perspective of authentication risks, risk vectors and risk mitigation principles and strategies, however, would go a long way towards improving the value of SP 800-63 to both government and private sector Trust Frameworks globally.

E. NIST has to bite the bullet and address the subject of biometrics directly. This set of technologies is expanding in the marketplace and will be a significant factor in multifactor authentication going forward. How to integrate biometrics into a multifactor implementation that satisfies NIST LOA is guidance that is very much needed.

F. Normalizing NIST IAM principles with federal bank audit requirements would be welcome.

G. More extensive discussion of compensating controls and what constitutes adequate implementations of same is needed in SP 800-63.

II. Structured Comments

A. What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction?

1. The Federal PKI architecture is a highly effective schema for establishing and asserting high degrees of identity assurance for protecting sensitive data such as PII and high-value business transactions. There currently exists a broad web of interconnected trust web based on X.509 technology as implemented under both the US Federal PKI Policy and the ETSI Qualified Certificate Profile.

2. The CA/Browser Forum has done an effective job in addressing the implementation baseline requirements for encryption certificates.

3. The FICAM policy and profile schemas for userID/password, SAML and OpenID 1.0 are useful and have seen general adoption, particularly on the identity proofing side.

4. Identity assurance initiatives in the Social Web have fared poorly in contrast. Significant policy and technology initiatives such as Google 2FA and FIDO Alliance are noteworthy exceptions with little broad-based impact. Google, Yahoo and other social media credentials have been widely federated, however, there continues to be little or no assurance of identity, security, privacy or trust in these credentials and the federation they operate within continues to be low-to-zero risk. Privacy protections are notoriously absent in this space.

B. How do they differentiate trust based on risk?

1. Federal PKI, FICAM non-PKI and ETSI/EU Regulation 910/2014 models are all, to one extent or another, based upon a risk vector – risk mitigation model. These models could be better aligned but there is broad agreement on the general concept. Social web models do not seem to differentiate trust in any generalizable manner, though it should be noted that Google's thinking in implementing its 2FA credential parallels the risk-mitigation approach.

C. How is interoperability of divergent identity solutions facilitated?

1. At the present time, interoperability of divergent higher assurance identity solutions exists only within the domains of federations or trust frameworks where policy and technology profiles can be defined explicitly. Even within these frameworks federated gateways or federated gateway components of web portals are required to be implemented. This is not a bad thing, as they provide a common point for policy and profile control, for testing, for rule enforcement, for provision of extended services such as attribute management and offloaded Authorization. More globalized versions of federated gateways may easily be implemented after global alignments of policies, profiles and technologies has been accomplished. In other words, the federated gateway model is highly scalable and implementable either as a stand-alone middleware service or as part of a portal service.

D. Could identity assurance processes and technologies be separated into distinct components?

1. The term, "identity assurance processes" is too vague to address. Identity proofing and token management were decoupled in SP 800-63-1 and since then many providers of identity proofing services

have certified themselves under one or more of the FICAM Trust Frameworks. This is a measure of success. On the other hand, stand-alone token service providers have certified themselves under FICAM Trust Frameworks only in combination with identity proofing partners in order to present a full service CSP for certification.

E. If so, what should the components be and how would this provide appropriate level of identity assurance?

1. Identity Proofing, Token or Credential technology and CSP policy/practice are the currently-recognized components and these can take many forms. There exist metrics, standards, determinants and practice that inform the community of the risk vectors inherent in each and of the mitigations/compensating controls that are effective to minimize each. That said, an assertion of identity is created by the combination of the elements, not by any element by itself and the assurance of identity is only as reliable as the lowest assurance factor for any component. The risk assessment demonstrates which component presents the greatest risk, therefore, the level of identity assurance (derived from a standardized risk assessment) of the assertion is only as strong as the weakest element. With this in mind, it should be clear that approaches that aim to implement distinct assurance levels for each component (though they usually only include proofing and token technology) do not satisfy the risk assessment – risk mitigation model and leave ultimate determination of the extent of risk mitigation to the relying party to calculate. While such independence may be seen to be beneficial in some use cases, it undermines a broader interoperable trust model and thereby introduces trust disconnects in federated business processes.

F. What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

1. Remote identity proofing using high definition, encrypted video links seems like a useful avenue to pursue.

G. What privacy considerations arising from identity assurance should be included in the revision?

1. When addressing privacy requirements, NIST should make no requirements for which no technology implementations exist.

H. Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

1. Both Federal PKI and FICAM policies do a reasonably good job of requiring privacy-enhancing implementations. Aligning privacy initiatives with the EU Data Protection Regulation – and its imminent update – would be an effective enhancement while also contributing to enhanced global interoperability.

I. What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

1. By generalizing token or credential technology requirements to a standard assessment of risk vulnerabilities and mitigations, 800-63 could resolve this issue simply.

J. Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions?

1. There can be no confidence levels in attributes. Relying Parties either choose to consume an attribute or they do not. For the sake of simplicity, we can consider that a Relying Party receives an extended attribute from one of two entities: either the authoritative issuer of the attribute or a retransmitter of the authoritative issuance. It would be appropriate to create guidelines for retransmitters, however, there is no reasonable way to create guidelines for authoritative issuers without unduly constraining that function (and that would lead immediately to the failure of such a guideline).

2. It is not at all clear that outsourcing authorization decisions is a good idea from the perspective of risk assessment and risk mitigation. The whole process of consuming extended attributes requires a separate risk assessment – risk mitigation effort.

K. What form should that representation take?

1. Representation of the confidence level of an extended attribute should be binary: either Reliable or Not Reliable. What steps determine the reliability of extended attributes should be part of the policy of each RP, RP proxy, Federation or Trust Framework.

2. It is the responsibility of the recipient of an extended attribute to determine for itself the reliability of the received attribute. It is not the responsibility of the attribute issuer to do so.

L. What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

1. Refer to the Third Deliverable of the OASIS Trust Elevation TC. The simple algorithm Reduced Risk = Increased Trust underlies thinking about Trust Elevation. Again, speaking in general terms, the way to reduce risk, and therefore elevate trust, is to mitigate a risk vector not addressed by the original identity assertion through a subsequent exchange. As previously noted, all elements of a credential issuance process – identity proofing, credential method or technology and process management – can be assessed from the perspective of risk vectors and mitigations. In fact, credentials from federation or trust framework members have already been pre-vetted along these lines, making it relatively easy for a Relying Party or its proxy to identify unmitigated risk vectors and implement mechanisms for acquiring assertions that fill the gap and thereby elevate trust. This process is more or less the core of the way the US financial services industry satisfies federal requirements for high assurance and privacy in online banking.

2. Performance metrics for Trust Elevation can most profitably be garnered from the financial services industry.

Federal Reserve Bank

In response to the National Institute for Standards and Technology request for comments, our comments responses have been ordered by the framing questions posed by NIST. Please consider the following:

1. What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

1.1 Use of OMB 04-04 as the sole means of determining assurance levels is does not support consistent application of authentication rigor across an enterprise. The next revision of 800-63 should expand the assessment outline provided in 04-04. A standard risk assessment process, like that encouraged by 800-30 should be adapted to this use case and adopted in 800-63.

2. Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

2.1 Interoperability between IT systems and the tendency to consolidate authentication processes both create a strong tendency to drive assurance levels to 4 across large swaths of the enterprise. The exclusive use of the high water mark concept for determining the assurance levels should be reconsidered.

> *Page 26:*
> *The low watermark is the basis for the overall level because the lowest level will likely be the target of the Attacker. For example, if a system uses a token for authentication that has Level 2 assurance, but uses other mechanisms that have Level 3 assurance, the Attacker will likely focus on gaining access to the token since it is easier to attack a system component meeting assurance Level 2 rather than attacking those meeting assurance Level 3. (See Sections 5 through 9 for information on assurance levels for each area.)*
>
> The above assumes that the likelihood of a threat being exploited across any part of the architecture is equal, in all cases, for all environments and all organizations. It also assumes that the consequence to any organization is the same.
>
> Threats to any architectural component, specifically those listed below, could be addressed separately and assigned a unique assurance level.
>
> - Registration and identity proofing process
> - Cryptographic credential form factors (USB Tokens or Card ICC) and the tie in for FIPS 104-2 Levels of cryptographic boundary certification
> - The binding between the identity proofing (LOA) and the hardware credential certificate policies

- Authentication protocols
- Token and credential management processes

Note the discussion of Kerberos on page 98 acknowledges that the strength of the protocol allows for LOA 4. A similar listing of commonly deployed technologies, their LOA (given some documented requirements) would be a useful addendum.

2.2 Revise section 4.8.Calculating the Overall Authentication Assurance Level with a specific example illustrating the low watermark principle. Also speak to how each part of the process contributes to the overall assurance level.

Each of the components are comprised of elements that have minimum thresholds to achieve the target assurance level for that component. Break out those elements and the minimum thresholds for each assurance level. A table might serve as a good format to summarize all of that information.

To more directly answer the framing question posed by NIST, the components are in the document now, but could be broken out more explicitly so that assurance level calculations could be applied to more clearly indicate the composite assurance level of the end-to-end service (using the low watermark principle).

Components include:
1) Registration and Issuance {section 5}
2) Tokens {section 6}
3) Authentication Process {section 8}
4) Assertions {section 9}
5) Token and Credential Management {section 7}

Each of the component areas should be further broken out to include elements that make up that component which contribute in some fashion to the overall assurance. We frequently refer to hardware tokens as a level 4 assurance token, but without satisfying the necessary elements of each of the components noted above that token is effectively reduced to some lower level of assurance (low watermark).

2.3 Is there a plan to incorporate derived credentials and some of the suggested or proposed physical token types described in Special Publication 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials? Could the token types described therein be mapped to Levels of Assurance?

3. What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

3.1 Can e-passports be used as a token for authentication directly? If so, at what authentication assurance levels?

E-passports have been in use since 2006. There are known processes for identity proofing, credential (and token) issuance, prevention and detection of electronic and physical tampering, use of the token and life cycle management. It seems that the elements are there to be evaluated for assurance levels. Could e-passports be added to the mix of acceptable authentication methods and mapped to an authentication assurance level?

In a similar vein, can EMV chip and pin cards potentially be used as an authentication token for other than financial/retail transactions (perhaps in combination with contextual factors)? See the Anil John blogpost at https://blog.aniljohn.com/2014/11/rfi-emv-enabled-debit-cards-as-authentication-tokens.html for more on this idea. If so, at what authentication assurance levels?

With either of these (especially with chip and pin EMV debit card) there is an increased level of confidence supported by a (potentially remote) electronic validation of the token itself which is bound to the bearer with some level of confidence that the holder/subscriber will have incentive to maintain control and protect the integrity of the token and credential.

3.2 It seems that this question may be related to the methods of "trust elevation" which would be used as additional authentication components. In this case, the "trust elevation" would be in the context of remote identity proofing specifically.

Dynamic knowledge based authentication, such as questions with multiple choice response regarding the bank which originated a loan to you in a specific timeframe, could be used to increase confidence in remote identity proofing. Additionally, reply to an SMS or text message with a specific verification code from a cell number verified to be associated with your name could be used in a similar "trust elevation" interaction which could increase the confidence in remote identity proofing.

4. What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

4.1 How are you accounting for the privacy components? At what levels of assurance is anonymous (privacy preserving capability) authentication appropriate? Would the service only need to know that you are authorized without requiring PII details?

4.2 The use of dynamic knowledge based authentication (even as a "trust elevation" mechanism) could present privacy concerns as public searches for intimate data (perhaps not rising to the standard for PII) which is part of a digital footprint are compiled as a source for comparison. This is mentioned as a caution without a suggestion for remedy as that can be extremely complex. The note here is that parts of our digital footprint may be gathered without consent and aggregated to support a legitimate and

user desired function, but may be surprising to the user when used in a different context than the one the data was provided or released to initially.

4.3 Location as a context factor to increase assurance of authentication, especially when used in a mobile context, could give users a sense of unease grounded in the perception (whether true or not) of personal location tracking and the associated privacy concerns.

5. What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

5.1 In addition to appendix B, develop another matrix that maps policy standards and assurance levels across commonly adopted credentials recommended by NSTIC.

5.2 The role of the Sponsor/Sponsorship and its relationship to the Applicant, Subscriber and Claimant is not discussed in the document. It would be helpful to include some mention of how the Sponsor contributes to the process.

6. Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

6.1 Yes, establishing confidence levels or guidance in estimating or calculating confidence levels of attributes which follow minimum standards for that attribute representation would be very helpful in making and supporting authorization decisions, especially when they support privacy preserving methods. This is a question that might be considered for NIST SP 800-162 *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* SP 800-162 should be referenced in SP 800-63 when revised.

> The guidance suggested above might begin with establishing an estimate of confidence level for the biometric(s) used in the e-passport which are detailed in the ICAO standards. This could then be extended to arrive at confidence levels for other biometric attributes and standards for representation of those attributes.

7. What methods can be used to increase the trust or assurance level (sometimes referred to as "trust elevation") of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

7.1 Update section 8.2.3. Throttling Mechanisms with additional acceptable environmental factors such as time of day, geographic location, system or OS fingerprinting information which is easily captured by the system and appended to other authentication information.

7.2 Will NIST address dynamic authentication methods or factors such as knowledge based authentication (KBA) or dynamically generated context factors in any sections other than 8.2.3. Throttling Mechanisms?

8. Additional Comments beyond the framing questions

8.1 Regarding multi-factor authentication

If the claimant responds to multiple pre-registered questions, is that considered single or multi-factor. In other words are multiple "something you know" considered single or multi factor? Or is multi factor only considered if the factors are of a different type?

Here are some other examples. If a claimant provided a fingerprint and an iris scan is that 1 or 2 factors? How about if a user provided multiple password – 1 or 2 factor?

Current definition

Multi-Factor	A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.

The definition of multi-factor should specifically address the cases described above. For example:

Case 1 definition – different factors

Multi-Factor:	A characteristic of an authentication system or a token that uses more than one authentication factor of different types. For example something you know and something you have. The three types of authentication factors are something you know, something you have, and something you are.

Case 2 definition – any combination of factors

Multi-Factor:	A characteristic of an authentication system or a token that uses more than one authentication factor of any type, including the same type. For example, something you know and something else you know would be valid. The three types of authentication factors are something you know, something you have, and something you are.

8.1.1 Multi-Stage Authentication Using Tokens

According to this section Multi-stage authentication is not considered multi-factor

"Multi-stage authentication processes, which use a single-factor token to obtain a second token, do not constitute multi-factor authentication. The level of assurance associated with the compound solution is the assurance level of the weakest token."

There is at least one multi-stage authentication scenario using tokens that we know of that could be considered multi-factor. For example, the process employed by one commercial financial institution is as follows:

1. A customer logons to the Bank website and authenticate using a password (***something I know***)
2. Upon successful logon the customer is prompted for a destination for a destination to receive an access code – a phone number or email address (***something I have***)
3. Upon entering the correct access code (***OTP- something I know***), the customer is granted access to her account information. The access code is only valid for 15 minutes

8.2 Threats and Mitigations

The document could be made more concise, and easier to follow and comprehend if the threat and mitigation tables were combined.

For example Table 1 (Registration and Issuance Threats) has columns labeled “Activity”, “Threat/Attack” and “Example”. Table 2 (Registration and Issuance Threat Mitigation Strategy) has corresponding columns labeled “Activity”, “Threat/Attack” and “Mitigation Strategy”.

I suggest that the tables be combined so that there are four columns. The columns would be labeled “Activity”, “Threat/Attack”,” Example” and “Mitigation Strategy”. I believe doing so would make it easier to make the association of mitigation strategies to threats/attacks. The same recommendation applies tables 4/5 and 8/9

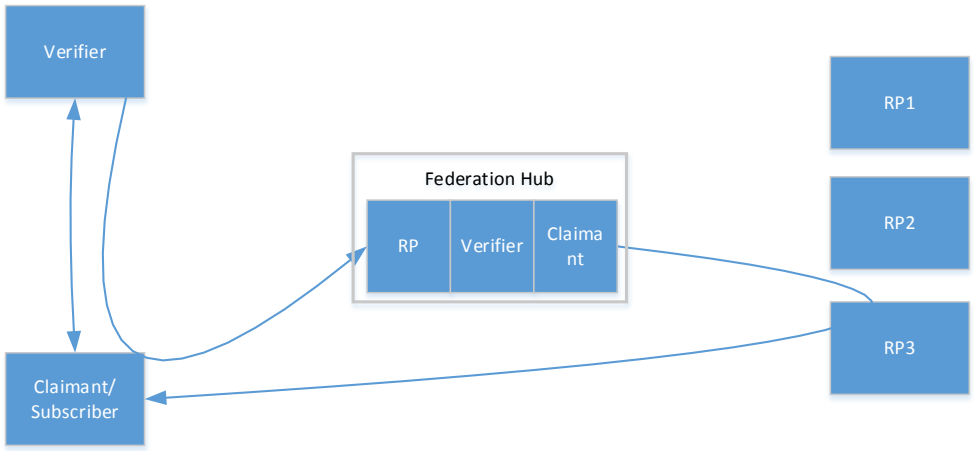
8.3 Assertion

Could a model that included a federation hub be included? The federation hub would act as a go between a subscriber and an RP allowing an organization to create a single federation trust and have it act in a transitive manner to several RPs.

The federation hub would play the role of an RP to a subscriber on the frontend, a verifier in the middle, and a subscriber to an RP on the backend

For example:

1. A subscriber obtains an assertion from their local verifier
2. The subscriber/claimant uses the assertion to authenticate to the federation hub.
3. The federation hub then creates an assertion that identified the original claimant and sends that to the final RP for authentication
4. The Claimant then has access to the RP



Clare Nelson

Dear NIST,

First, I applaud your work. As a consultant I get paid to be critical. As a CISSP and member of ISSA and OWASP, my passion and commitment is to make it harder for the bad guys, and protect innocent people.

Second, there is far too much jargon. There is a growing chasm between the NIST definition and the various interpretations of various MFA vendors:

- Multi-Factor Authentication
- Two Factor Authentication
- Multi-Modal Authentication
- Strong Authentication
- Advanced Authentication (Gartner)
- Two-Step (Apple)
- Login Approvals (Facebook)

Third, my recent authentication research includes analysis of 200+ authentication vendors for a large client. My work has been, and will be, presented at the following venues:

Speaking Engagements: Multi-Factor Authentication

- March 2015: Austin BSides information security conference
- May 2015: FIS Global, a Fortune 500 financial services firm, a WebEx for the global team, here are the slides: http://www.slideshare.net/eralcnoslen/financial-services-20150503
- **Paper accepted: September 2015, OWASP AppSec USA, San Francisco**
- Pending acceptance: International ISSA conference, Chicago, October 2015
- Pending acceptance: Gartner IAM Summit, Las Vegas, December 2015

Journal Publications: Multi-Factor Authentication

- **Feature article for Information Systems Security Association (ISSA) Journal, April 2015,** *Multi-Factor Authentication: What to Look For, http://www.bluetoad.com/publication/?i=252353*

Attached is a copy of my ISSA Journal article, *Multi-Factor Authentication: What to Look For*.

My suggestions are as follows:

- Revisit the history, and definition of MFA, especially in light of IoT, and things we cannot even imagine today.
- Raise the bar for the Achilles heel of MFA, account recovery. This is also a major vulnerability.
- Create a new category for biometrics, and specify they are acceptable as an additional factor. Biometrics are a good username; not a password. There is nothing secret about my fingerprints

on a coffee mug, my face math on Facebook and LinkedIn, or my voice as recorded by any financial institution I call.

- Follow FFIEC guidelines. Two-factor is insufficient. BioCatch collects 400 parameters.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Clare Nelson, CISSP

Attached: (PDF) Multi-Factor Authentication: What to Look For, by Clare Nelson

IRS

Below are my commendationsŠ

Executive Order 13681

· Financial transactions would be required to be at LOA 3 or higher (both higher Identity Proofing standards and multifactor authentication)

Examples:

- Payments
- Viewing of any financial data including transaction history
- Viewing of tax transcripts

· Must establish User IDs and Passwords - no guest or on time access

Strengthen LOA C require additional Identity proofing controls on top of the current requirements (name, address, date of birth, government id or financial validation)

Tom Jones

My comments follow each point. If you have further questions, please let me know.

- What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

  This question conflates authentication and authorization. Risk evaluation should not be determined during authentication as the value of the asset to be protected is not known. Identity is captured in commercial web sites from the very first contact. Often a series of web pages are viewed before the user is asked to enter credentials and by that time there is typically a good deal of identity information already collected.

- Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

Yes – the collection of attribute information should be one processes. At the time that access to a valuable asset is made a high speed evaluation of the risk must be made in a time frame consistent with user expectations. After the fact the access decision should be evaluated with others, typically when traffic levels are lower. The best sort of access provision is one that can be revoked later if additional evaluation warrants it.

- What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

Sorry, but specific metrics are: 1> confidential, 2>constantly changing based on experience. It is our experience that this is not an appropriate topic for standardization.

- What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

See the following page on the IDESG web site.
https://www.idecosystem.org/wiki/Privacy_Enhancing_Technologies

- What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

The description of the four levels are not helpful. ID is just another attribute, it comes with sub attributes, so a list of the attributes of the identity would be most helpful to a risk evaluation. Like, is the private key protected with hardware? Was in-person proofing required? What sort?

- Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

Yes – the simplest is just a percentage. 1% to 99%

- What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.

Please see the following page on the IDESG web site.

https://www.idecosystem.org/wiki/Trust_Elevation_Use_Case

SP 800-63-2 – Includes the following text appropriate to the use of Biometrics. TSI's comments are highlighted in yellow

1) This document supports the use of biometrics to "unlock" conventional authentication tokens, including passwords to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process. …..This implies that biometrics can be used to unlock passwords. It might be useful to make that clear in the statement.

2) More generally, something you are ("something you are" is misleading in the context of a biometric sample – "something about you" might more accurately describe a biometric sample) does not generally constitute a secret. Accordingly, this recommendation does not permit the use of biometrics as a token. The word "generally" does not mean exclusively. Where biometrics are secrets (e.g. in the Crypto-Sign® biometric process, where the sample is a secret sign made upon the screen of mobile device, without ink feedback) the restriction on its use should be lifted and it would be useful to emphasize that. I don't think the current language is strong enough in that regard.
3) This publication recommends that biometrics be used in the registration process for higher levels of assurance to later help prevent a Subscriber who is registered from repudiating the registration, to help identify those who commit registration fraud, and to unlock tokens. But this should not be the only recommended use and the statement should clarify that.
4) At Level 2: For electronic transactions, the Applicant shall identify himself/herself in any new transaction (beyond the first transaction or encounter) by presenting a temporary secret or biometric sample which was established during a prior transaction or encounter, or, in the case of a secret, sent to the Applicant's phone number, email address, or physical address of record. For physical and electronic transactions, the Applicant shall identify himself/herself in person by either using a secret as described above, or by biometric verification (comparing a captured biometric sample to a reference biometric sample that was enrolled during a prior encounter).
5) At Level 3: For electronic transactions, the Applicant shall identify himself/herself in each new electronic transaction by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or physical address of record, or the applicant shall identify himself/herself using a biometric sample matched against a previously enrolled biometric template. Permanent secrets shall only be issued to the Applicant within a protected session. For physical transactions, the Applicant shall identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter. Temporary secrets shall not be reused. If the CSP issues permanent secrets during a physical transaction, then they shall be loaded locally onto a physical device that is issued in person to the Applicant or delivered in a manner that confirms the address of record.
6) The CSP may issue a derived level 4 credential for a suitable Level 4 capable token, based on an original level 4 credential. Before issuing the derived Level 4 credential, the CSP shall: • Obtain and verify a copy of a biometric (template or sample and if a template, how is it verified? If a sample, what is it verified against?) recorded when the original credential was issued. An example of such a biometric (biometric what?) is the signed biometric data object on a PIV card, however if the biometric reference is not available from the Level 4 token, it may be obtained

elsewhere, as long as its authenticity is assured; • Compare a fresh biometric sample obtained in person from the Applicant to the reference biometric retained from the original Level 4 credentials and determine that they match, and; • Determine that the token that contains the token secret associated with the derived credential meets the requirements of Table 6 for a Level 4 token.

7) There are two optional inputs to the token: token input data; and token activation data. Token input data, such as a challenge or nonce, may be required to generate the token authenticator. Token input data may be supplied by the user or be a feature of the token itself (e.g. the clock in an OTP device). Token activation data, such as a PIN and/or biometric sample, may be required to activate the token and permit generation of an authenticator. Token activation data is needed when a Claimant controls the token through something you know or something you are. (Where the token is something you know, such as a password or memorized secret, token activation is implicit.)
8) Multi-factor Token – A token that uses two or more factors to achieve authentication. For example, a biometric sample plus a PIN or a private key on a smart card that is activated via PIN is a multi-factor token. The smart card is something you have, and something you know (the PIN) is required to activate the token.
9) Multi-factor (MF) One-Time Password (OTP) Device – A hardware device that generates one-time passwords for use in authentication and which requires activation through a second factor of authentication. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric sensor (e.g., fingerprint reader or a screen with graphical input) or a direct computer interface (e.g., USB port). The one-time password is typically displayed on the device and manually input to the Verifier as a password, although direct electronic input from the device to a computer is also allowed. The token authenticator is the one-time password. For example, a one-time password device may display 6 characters at a time. The MF OTP device is something you have, and it may be activated by either something you know or something you are.
10) Something you are (about you?) may be replicated. An Attacker may obtain a copy of the token owner's fingerprint and construct a replica - assuming that the biometric system(s) employed do not block such attacks by employing robust liveness detection techniques. (There is a general spoofing threat with all biometric modalitities – some are a greater threat than others)
11) Token Threat/Attack Threat Mitigation Mechanisms Theft - Use multi-factor tokens which need to be activated through a PIN and/or a biometric sample. Duplication - Use tokens that are difficult to duplicate, such as hardware cryptographic tokens. Discovery - Use methods in which the responses to prompts cannot be easily discovered. Eavesdropping - Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. - Use tokens that generate authenticators based on a token input value. - Establish tokens through a separate channel. Offline cracking - Use a token with a high entropy token secret - Use a token that locks up after a number of repeated failed activation attempts. Phishing or pharming - Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. Social engineering - Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. Online guessing - Use tokens that generate high entropy authenticators.
12) MF Hardware Cryptographic Token Level 4 Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher.22 Shall require the entry of a password, PIN, and/or biometric sample to activate the authentication key or password. Shall not allow the export of authentication keys.

13) The principles used in generating Table 7 are as follows. Level 3 can be achieved using two tokens rated at Level 2 that represent two different factors of authentication. Since this specification does not address the use of biometrics as a stand-alone token for remote authentication, achieving Level 3 with separate Level 2 tokens implies something you have and something you know: Token (Level 2, something you have) + Token (Level 2, something you know) → Token(Level 3) In all other cases, combinations of tokens are considered to achieve the Level of the highest rated token. (will need changes if you include some of the suggested changes above)

Joe Wodzinski

Anything that can be done to minimize the number of passwords required to maintain and periodically update would be beneficial. Being able to use our identification cards for authentication purposes has proven beneficial logging in to a couple of PBS programs that I use such as RETA and EASI. It would be nice if it could be applicable to many of the other sites that I routinely use such as GSA OLU or UPPS (utility profile payment system), or any other government related site requiring a user name and password.
I think we are headed in the right direction and thank you for the information.